Enterprise iSCSI SANs

Windows IT Pro

A PENTON PUBLICATION

OCTOBER 2012 | WINDOWSITPRO.COM | WE'RE IN IT WITH YOU

Windows Server 2012 and Windows 8 Arrive

Hiding Data in Active Directory

Exchange Server 2010 SP2
Deconstructing the Hybrid Configuration Wizard

PowerShell
Overcome Schtasks Limitations

Top 10
Microsoft Surface FAQs

Cloning Virtual Domain Controllers

Plus >>

CLOUD TRANSFORMS IT

EMC²

OCTOBER 2012 / VOL. 18 / NO. 10

COVER STORY ▼

Introducing Windows Server 2012

— Michael Otey and Sean Deuby

Get a first look at some of the most useful features and enhancements in the new Windows Server OS release.

36

Welcome to Windows 8

— Paul Thurrott

Windows 8 might just be a game changer. Find out how the new client OS could change the way you use Windows—permanently.

54

Features

62 **Enabling List Object Mode in a Forest**
Guido Grillenmeier

73 **Deconstructing the Hybrid Configuration Wizard in Exchange Server 2010 SP2**
Jorge R. Diaz

89 **Updating a Scheduled Task's Credentials**
Bill Stewart

Special Features

52 **Microsoft Releases Windows Server 2012**

60 **Microsoft Windows 8 Arrives**

Interact

28 **Ask the Experts**

In Every Issue

116 **Ctrl+Alt+Del**

117 **Advertiser Directory**

117 **Directory of Services**

117 **Vendor Directory**

Chat with Us

Facebook Twitter LinkedIn

Access articles online at www.windowsitpro.com. Enter the InstantDoc ID (located at the end of each article) in the Search box on the home page.

Columns

7 IT Pro Perspectives
Microsoft's Summer of Love
B. K. Winstead

10 Need to Know
Windows 8 and Server 2012 Schedule, Why Metro Is a No-No, and a New Mouse
Paul Thurrott

16 Windows Power Tools
Automating PowerShell Reports, Part 1
Mark Minasi

20 Top 10
Microsoft Surface FAQs
Michael Otey

24 Enterprise Identity
Cloning Virtual Domain Controllers in Windows Server 2012
Sean Deuby

Products

95 **New & Improved**

99 **HP ProLiant DL380p Gen8**
Michael Otey

103 **Idera SharePoint encrypt**
Russell Smith

107 **Enterprise iSCSI SANs**
Michael Dragone

110 **Industry Bytes**

Windows IT Pro, October 2012, Issue no. 218, ISSN 1552-3136. *Windows IT Pro* is published monthly by Penton Media, Inc.

Windows IT Pro, 748 Whalers Way, Fort Collins, CO 80525, 800-621-1544 or 970-663-4700. Customer Service: 800-793-5697.

We welcome your comments and suggestions about the content of *Windows IT Pro*. We reserve the right to edit all submissions. Letters should include your name and address. Please direct all letters to letters@windowsitpro.com. IT pros interested in writing for *Windows IT Pro* can submit articles to articles@windowsitpro.com.

Windows IT Pro

vmware

Continue your journey to the cloud with VMware Workstation 9.

With powerful new features including best in class Windows 8 support, we're transforming the way you work with virtual machines. A new web interface allows you to access virtual machines running on a PC or the datacenter from a tablet, smart phone, or PC. You can also create and send virtual machines that are encrypted, limit USB devices and have locked settings to anyone in your organization.

VMWARE WORKSTATION 9

Buy Now »

Microsoft's Summer of Love

Does the unprecedented number of major product releases in 2012 represent a total renaissance or last hurrah?

We don't often look to Microsoft to make a lot of news during the long, hot summer months. However, the summer of 2012 has seen Microsoft making announcements and releasing products with Olympic swiftness. But this is no game for the company. The stakes are high, and the company's sights are perhaps even higher.

It's not just the timing of these releases. We've also never seen a wave of so many Microsoft product and service releases in so short a time span. Essentially, the company has released new versions—either shipping or in beta (or "Preview")—of every one of its major product lines over the course of about two months. Windows 8 and the Office 2013 suite have gotten the Microsoft love in terms of flashy launch events, while the server products of greatest interest to IT pros, such as Windows Server 2012, SharePoint 2013 Preview, and Exchange Server 2013 Preview, have been revealed lying on the beach only after the waters recede.

The consumer focus isn't just about launch events, either; it's ingrained in the product releases themselves. Much has been written about the Windows 8 Metro-style interface (which I know we're not supposed to call Metro anymore, but—tough), which is optimized for tablets and touch screens—but that means it's rather ahead of the curve for most IT shops. And to coincide with Windows 8's debut, Microsoft announced its own tablet line, the Microsoft Surface, to compete with the iPad and jumpstart the Windows 8 tablet market.

B. K. Winstead

is a senior associate editor for *Windows IT Pro*, *SQL Server Pro*, and *SharePoint Pro*, specializing in messaging, mobility, and unified communications.

Email

Twitter

Blog

It seems a peculiar strategy for Microsoft to effectively ignore the business software that has been the company's lifeblood and focus instead on promoting consumer releases.

As part of the Office 2013 launch, Microsoft introduced a new subscription plan for Office 365 aimed at home users, Office 365 Home Premium. The service gives home users the full Office experience—Word, Excel, PowerPoint, Outlook, OneNote, Publisher, Access—in a portable form, with your documents stored in SkyDrive for anywhere access. Shortly after the Office launch event, Microsoft announced a complete overhaul of Hotmail, with the rebranded free email service called Outlook.com. The clean UI of the web service and the company's messaging around this service is clearly designed to take on major competitor Google Gmail directly.

In many ways, it seems a peculiar strategy for Microsoft to effectively ignore the business software that has been the company's lifeblood and focus instead on promoting consumer releases. By comparison, in past release cycles, the business-focused products such as Windows Server, Exchange Server, and SharePoint have warranted their own individual launch events or special promotion from Microsoft. Yet this time around, for instance, the Exchange Server 2013 Preview was available for download for a full week before the Exchange Team Blog ever made any announcement about its availability.

This shift could almost appear to be an act of desperation, a company trying to make waves in the consumer space, to be cool and sexy like certain of its competitors—even though this is a realm in which Microsoft has largely failed miserably in the recent past. An August 2012 *Vanity Fair* article has been getting a lot of attention for talking about "Microsoft's Lost Decade" and suggesting that the only solution for the company is to split into pieces because it's become too diverse.

So, is this consumer push just Microsoft's last hurrah, a last attempt to achieve relevance in a technology space that's increasingly being led by consumer products? Or does Microsoft's strategy signal a renewed energy and understanding of both the competition the company faces and the way consumers—and, by extension, businesses—are using technology?

We've been talking about the "consumerization of IT" and the related concept of bring your own device (BYOD) for several years now. It's certainly no surprise to IT pros, therefore, that the consumer space has been driving adoption of technology in business environments. In smartphones, we've seen BYOD work to the great benefit of Android and iPhone—and huge detriment of RIM BlackBerry. In tablets, the iPad quickly insinuated itself in the hands of employees and IT pros. Why wouldn't Microsoft want to duplicate that success with its own branded Surface tablet and Windows 8? Get consumers loving it and then asking their workplaces to purchase or support them for business use.

Office 365 seems to be another forward-looking step. For years, Microsoft has relied on product cycles for its revenue—releasing new versions of its successful product lines and convincing consumers and businesses to buy those new versions every two or three years. Moving to a services model gives the company a steady, subscription-based income. And focusing on consumers in this space helps to capture the mindshare of users even before they have to make technology choices in business. One of the stumbling blocks for cloud computing generally has been a fear of giving up control of systems and data; but if your workforce and IT pros are already familiar with using a Microsoft service in their non-work life, how much easier does that make it to choose Microsoft's service for work as well?

Microsoft has often been criticized for moving too slowly, not seeing the new directions and trends in the marketplace until after competitors have blazed a trail. Certainly you can look at areas such as smartphones and tablets and see truth in that analysis. However, it's just possible that this recent onslaught from Microsoft, this tsunami wave of releases focused on the consumer, signals a new understanding of what it takes to compete today and how to maintain relevance even in the business sphere. As the betas and Previews become shipping products and services over the coming months, we'll see if Microsoft's summer of love is a true renaissance for the company, or a washout. ■

InstantDoc ID 144109

Windows 8 and Server 2012 Schedule, Why Metro Is a No-No, and a New Mouse

Paul Thurrott

is senior technical analyst for *Windows IT Pro*. He writes the SuperSite for Windows, a weekly editorial for Windows IT Pro UPDATE, and a daily Windows news and information newsletter called WinInfo Daily UPDATE.

Email

Twitter

Website

There's so much going on this month, I had to go back and do a double-take at last month's column because I was sure I had skipped a few months. So let's get right to the heart of the matter: scheduling and details about Windows 8, Windows RT, and Windows Server 2012.

Windows 8 Is Done . . . But It's Never Really Done

On August 1, 2012, about two weeks after it had actually completed development of Windows 8, Microsoft formally announced the completion of its next desktop OS. Actually, Windows 8 is a hybrid mobile and desktop platform, a point I'll make more completely in my coming review. Microsoft actually has a lot riding on this one. It all has to do with the rapidly changing wants of consumers, which are a larger and more fickle audience than the business-user base that Microsoft wrapped up years ago. With Apple selling more iPads each quarter, the software giant arrived at the same conclusion as industry analysts did, for a change. And Windows 8 is its response.

We will be debating the merits of Windows 8 for months to come. For now, I'd like to focus on the point of this column—literally, what you need to know—and provide you with some important information about Windows 8 (and its ARM-based stablemate, Windows RT).

Windows 8 Release Schedule

Microsoft announced that it would make Windows 8 generally available on October 26. It will ship in a retail Upgrade version only—there are no more Full versions because all customers now qualify for

upgrade pricing—in both electronic and disc-based retail packaging. It will also be available with new PCs (Windows 8) and devices (Windows RT) at that time. The Windows RT–based version of Microsoft's Surface tablet will also ship on that date, with the Windows 8 versions arriving 90 days later. No word on Surface pricing.

Windows RT Device Pricing

Windows RT remains a dark horse. The technical tradeoffs are well understood, even though no one outside of Microsoft has one of these devices. They should be thinner and lighter than equivalent Intel-type, Windows 8 PCs, and they should get better battery life. But Windows RT devices can't run legacy desktop applications—a cute way of saying "every single Windows application ever developed by third parties, and most applications developed by Microsoft, too." So predictions about this platform are all over the map.

Also all over the map are theories about how Microsoft's partners intend to price Windows RT devices, although the most popular theory is that device makers are courting disaster if these things come in any higher than an iPad. Having seen the price list for third-party Windows RT devices—sorry, I can't go into details yet—I can report that there's nothing to worry about. And I'd remind you that the price range of Apple's beloved iPad is $499 to $830. Got it?

The question is whether Windows RT devices represent a better value proposition than the iPad. With Windows 8, you can at least argue that the devices, while heavier, louder, and less elegant than the iPad, at least run real Windows applications. With Windows RT devices, you get Office 2013. But it's a low-end version of Office (Home and Student), and it doesn't run any other real Windows applications.

Metro Naming

One of the odder things about Windows 8 is that its architects refused to name certain key components of the OS. This led to some bizarre exchanges I had with people at Microsoft who professed to not

understand the uproar (I was writing a book about Windows 8 and thus needed to name components). But one of the terms Microsoft did use with Windows 8 during development was Metro, a design language that was first used in the development of Windows Phone but has since cropped up in virtually every major Microsoft platform, including Windows, Windows Server, Office, Xbox, the web, and more.

With Windows 8, Microsoft refused to name the new Windows Runtime (WinRT)–based environment "Metro," although the company referred to the apps that run in that environment as "Metro-style" apps. And so most people, myself included, referred to this new environment as Metro. This made sense, and it still does. Except for one thing.

Within days of the completion of Windows 8, a chilling memo made its way through Microsoft and to its partners. The Metro name, it turned out, isn't owned by Microsoft, and Microsoft has been legally threatened by a company it refuses to name—Germany's Metro AG, obviously—and has ordered the troops to stop using it. Although Microsoft has many names in reserve—including "Modern," the original code name of Metro—that it could use instead, it has decided, bizarrely, to do the wrong thing.

Microsoft has decided that Metro will simply be called the Windows 8 UI—and that Metro-style apps will be called Windows 8 apps. In case it's not obvious, the reason this decision is wrong is that Windows 8 is a slice in time, a single version of Windows. The Metro environment—as I will continue to call it, sorry—will continue past Windows 8, to Windows 9 or whatever comes next. And it's already being used by multiple Microsoft platforms, as already discussed. This new naming scheme stinks.

New Mobile Mice and Keyboards

With Windows 8 and Windows RT, Microsoft is greatly expanding its long-running line of hardware peripherals by creating a new line of Surface tablets (and, presumably, other devices too, in the future). But Microsoft isn't ignoring its more traditional hardware lineups. In

addition to upgrading its existing Touch Mouse with Windows 8 gesture support, the software giant is also unleashing two new lines of mice and keyboards that are designed to fully take advantage of this new OS.

The Sculpt line is perhaps the least interesting, because the products—the Sculpt Mobile Keyboard and Touch Mouse—somewhat resemble existing products. But the keyboard features Windows 8 hot keys (for Charms and other system services), whereas the mouse includes a four-way touch scroll strip that's ideal for Metro apps.

More interesting is the new Wedge line, which consists of the Wedge Mobile Keyboard and Wedge Touch Mouse. Both feature stunning designs and will nicely complement any Windows 8 or Windows RT PC or device. The Wedge Mobile Keyboard includes Windows 8 hot keys and media keys, and a durable, snap-on cover. And the Wedge Touch Mouse looks like a work of art, with its cool wedge design. (No word yet on ergonomics.) You can find out more about these products in "Windows 8 Tip: New Mice and Keyboards" and in the accompanying Windows 8 photo gallery.

European Union Now Investigating Windows 8 and Windows RT

With both Google and Mozilla claiming that Windows 8 and Windows RT prevent them, in unique ways, from creating browsers that can offer the same technical features as Microsoft's Internet Explorer, antitrust regulators in the European Union (EU) have taken the bait. The EU announced in late July that it was investigating whether Microsoft is hiding capabilities from competitors, a situation that would put the software giant in contempt of its EU-based antitrust order.

Of course, Microsoft revealed this year that it was in contempt of this order already. Apparently that court-ordered browser ballot feature hasn't actually been included in Windows 7 since Service Pack 1 shipped, around February 2011. Oops!

So what's a little non-compliance between friends? Something tells me we're going to find out. I have a hard time imagining Microsoft

not changing Windows 8 to meet the needs of Google and Mozilla. Stay tuned.

To the Future: How Will Windows Be Updated?

Speaking of changing Windows 8, one of the dirty little secrets about Microsoft's next OS is that—surprise—it's not really done. See, those Metro experiences that we're supposed to call something else are very much a 1.0 product, and the state they're shipping in this year is very basic indeed.

Microsoft can't let Metro sit still for three years and, as it turns out, it won't. So that monolithic, three-year development cycle that Windows has been on since Steven Sinofsky took over has been tossed aside. And for the next few years at least, we're going to be dealing with a lot of updating.

The question, however, is what form these updates will take. (Service Packs? Feature Packs? Windows Updates?) Mr. Sinofsky announced this change to employees about a month ago in a heavily protected internal memo that I'm still trying to get my hands on. But based on the bits I've heard about, everything is changing. Whether things get back to normal with Windows 9 is unclear, although there's a credible theory making the rounds that suggests that Microsoft's real plan is to mature the Metro stuff enough so that the company can relegate the aging desktop interface to maintenance mode, then move forward, NT-style, with Windows RT.

If this vision comes to fruition, Microsoft might even re-imagine versioning, especially in the product branding, so that Windows 9/Windows RT would just be called Windows. The company is already doing this with online services: You never think of Windows Azure or Office 365 as version whatever. They're just Azure and Office 365.

Windows Server 2012 RTM and Release Schedule

Windows 8 wasn't the only product Microsoft finalized this past month. It also finished work on Server 2012, which was developed in

lockstep with Windows 8, although it will, oddly, roll out on a different, and quicker, schedule. Microsoft will make Server 2012 available to customers (via new servers and in software form) on September 4. The OS will ship in just two mainstream product editions, Windows Server 2012 Standard and Windows Server 2012 Datacenter, and two other editions, the low-priced but suddenly very versatile Windows Server 2012 Essentials and Windows Server 2012 Foundation, the latter of which will be made available only via new low-end server hardware purchases. (It's not clear if Essentials and Foundation are shipping September 4, however.)

Office 2013 Customer and Outlook.com Previews

Microsoft also shipped preview versions of two hugely important platforms recently: Office 2013—which encompasses online services (Office 365, Office Web Apps, and more), servers (Exchange Server 2013, SharePoint 2013, and more), and a new lineup of office productivity suites and applications—and Outlook.com, a gorgeous new Metro-style replacement for the aging Hotmail webmail service.

Office 2013 is almost too big to wrap one's mind around. Microsoft is embracing the cloud with this release, and the preferred installation type will be a Click-to-Run–based virtualized installation that takes just minutes to complete. Office 365 is being expanded greatly and will even include consumer-oriented versions. And it will come with Office 2013 now, with each licensed seat gaining access to five installations of the client suite. How's that for aggressive?

Outlook.com, meanwhile, is enough to make even diehard Gmail users switch, and although many of its features debuted quietly in Hotmail over the years, they'll be a revelation to new users. (And given how good this service is, I expect to see a lot of users.) You can read more about Office 2013 on my Microsoft Office landing page on the SuperSite for Windows. And I've got some tips about Outlook.com as well. ■

InstantDoc ID 143979

Automating PowerShell Reports, Part 1

Understanding send-mailmessage

Mark Minasi

is a senior contributing editor for *Windows IT Pro*, an MCSE, and the author of 30 books, including *Mastering Windows Server 2008 R2* (Sybex). He writes and speaks around the world about Windows networking.

Email

Twitter

Website

I want to take a short break from my in-depth look at PowerShell-based Active Directory (AD) query tools and show you how to put some of that query power to work in a concrete way. You've already seen that the command

```
search-adaccount -usersonly -accountinactive -timespan
  "90"|select samaccountname,lastlogondate|sort lastlogondate|ft
```

will generate a fairly useful list of domain users who haven't logged on in the past 90 days, sorted by how many days have passed since that last logon. It's of some value and not too ugly a command to remember, but who wants to have to open a PowerShell prompt and type it to get that information? This month and next, I'll show you how to get PowerShell to automatically generate that report daily and deliver it to you via email.

Before you can get there, however, you need a PowerShell cmdlet called *send-mailmessage*, because it's how you'll get PowerShell to send that report to your mailbox. Understanding its syntax is mostly trivial, but there are a few not-so-simple parameters, so here it is in parts. In its simplest form, *send-mailmessage* looks like

```
send-mailmessage -to joe@bigfirm.com -from sue@cogswellcogs.net
  -cc attorney@win2ktest.com -bcc covermybutt@cogswellcogs.net
  -subject "Looks good, let's sign it Tuesday at noon"
  -body "Let's meet at the Pungo Grill and ink this deal."
  -smtpserver po.cogswellcogs.net
```

It's a long line, but it's simple. Any SMTP client must, at minimum, allow you to specify those items. If you don't want to type the SMTP server's name, you can create a default one in your PowerShell profile. To do so, create a folder in Users*yourname*\Documents\WindowsPowerShell (if it doesn't yet exist). In that folder, create a text file named *Microsoft .Powershell_profile.ps1*. Open that file and add the line

```
$psemailserver=yourSMTPServer
```

as in

```
$psemailserver="mail1.bigfirm.com"
```

Finally, from the PowerShell command prompt, type

```
set-executionpolicy remotesigned
```

What you've done is modify or create your own PowerShell profile, a text file in which you can type commands that get automatically executed whenever you enter PowerShell (and yes, I've covered this before, but it's been a while). The *set-executionpolicy* command, which you need to type only once on your computer, gives your PC permission to run PowerShell scripts (and I'll cover that in greater detail in the future). Now, exit PowerShell and re-enter it to enable the new/modified profile, then type

```
$psemailserver
```

PowerShell will display your current default SMTP server. Before going any further, test that first *send-mailmessage* command, substituting some local-to-you accounts and the name or IP address of your local SMTP server. If it fails, it's because of your SMTP server's security. Mine is set up so that if a client is either connecting from

my internal subnet or providing domain credentials, it will send mail, so I needn't provide credentials. However, if your SMTP server wants credentials, just add *-credential username* and you'll be prompted for a password. (In the long run, you will, however, need to tweak your SMTP server's authentication requirements, because you'll ultimately want to schedule this command to run automatically.)

That syntax will work fine, but clearly the body that I specified was pretty basic—just one line and, yes, PowerShell wants you to somehow stuff the whole body of the message inline. Here are a few ways to do that.

First, if you have just a few short lines to type, you can indicate line breaks with the PowerShell "escape code" of `*n*—that's a backtick and a lowercase *n*. For example, here's a two-line body:

```
-body "Meet me at noon.`nI'll be waiting."
```

That would show up as two lines. Sometimes, though, you'll want to grab the contents of a file and have *send-mailmessage* use that as the body. You can do that with a cmdlet named *get-content* that essentially grabs the contents of a file and shows it onscreen. Typing

```
get-content test.txt
```

would show test.txt's contents. So, you'd think that putting that in parentheses would make PowerShell quite happy, as in

```
-body (get-content test.txt)
```

But what looks like text (or System.Text in PowerShell-ese) isn't exactly text; it's what .NET and PowerShell call a System.Object type of data. You can fix that by piping the *get-content* cmdlet into another cmdlet called *out-string* that—you guessed it—converts System.Object to System.String, making PowerShell happy, and then this works:

```
send-mailmessage -to joe@bigfirm.com -from sally@bigfirm.com
  -subject "Here's the report!" -body (get-content c:\files\
  report.txt|out-string)
```

You can shorten a line like that a bit with any of *get-content*'s three aliases: *cat, type*, or *gc*. Even better, if your file is HTML rather than text, then *send-mailmessage* will send it as HTML if you add the parameter *-bodyashtml*.

I think you can understand *send-mailmessage*'s usefulness and see why I fell in love with it as soon as I met it, but it's still missing two things. First, it would be nice to run a cmdlet and make that cmdlet's output the body text for an email message. Second, wouldn't it be cool if you could schedule *send-mailmessage* to run automatically? We'll do that next time. ■

InstantDoc ID 143953

Microsoft Surface FAQs

Learn more about the new tablet

Michael Otey

is senior technical director for *Windows IT Pro* and *SQL Server Pro* and author of *Microsoft SQL Server 2008 High Availability with Clustering & Database Mirroring* (McGraw-Hill).

Email

Microsoft's recent announcement of the Surface shows that the company has every intention of moving into the tablet market that formerly was the near-exclusive domain of the Apple iPad. I still remember those Steve Ballmer presentations where he expressed disdain for both the iPhone and the iPad, but nowadays, following the success of both of those devices, Microsoft has obviously reconsidered its position and decided to jump feet first into the phone and tablet markets. Unlike the strategy with the marginally successful Windows Phone, Microsoft has decided that it will compete with its own tablet device rather than relying on partners to bring the Surface to market. When you add up this news with the entry of Google's new Nexus 7, there's no doubt the tablet market will be a hot spot for 2013. Let's take a look at the top 10 frequently asked questions about the pending Surface.

1 What's the Surface form factor, and how does it compare to the iPad?

There are actually two versions of the Surface, and they're slightly different. Both versions provide a 10.6" HD touch screen. The Windows RT version of the Surface tablet is slightly smaller, measuring 0.366" thick and weighing 1.5 pounds. The Windows 8 version is 0.52" thick and weighs 2 pounds. These specs are similar to the new iPad, which has a 9.7" 2048 × 1536 display and is 7.31" wide by 0.37" thick. The iPad weighs in at 1.44 pounds.

2 What makes the Surface different from the iPad?

There's no doubt Microsoft has put some real thought into the Surface design. It comes with a convenient built-in kickstand. The Surface tablet also features a unique 3mm magnetically attached cover that uses pressure-sensitive technology to double as a keyboard and mouse. Early

reports say that the initial release of the Surface will have only WiFi connectivity and will lack the 3G/4G capabilities found in the new iPads.

There's no doubt Microsoft has put some real thought into the Surface design.

3 What processor does the Surface use?

The different Surface models will come with different processors. NVIDIA made public that the Windows RT Surface will use the NVIDIA Tegra ARM processor. This processor will probably be the Tegra 3, a 1.4GHz quad-core processor. The Windows 8 version is currently expected to use an Intel i5 CPU. The Intel i5 is used in many of today's ultrabooks—it's dual-core and runs at up to 2.7GHz. In comparison, the iPad uses a 1GHz dual-core Apple A5 processor that's manufactured by Samsung.

4 What sort of storage and connectivity options does the Surface have?

The Windows RT version will be available in 32GB and 64GB. Connectivity options include Micro HD Video, microSD, USB 2.0, and twin 2 × 2 MIMO antennas for WiFi. The Windows 8 version will come in 64GB and 128GB and will have a microSDXC, USB 3.0, Mini DisplayPort Video, and 2 × 2 MIMO antennae.

5 Is the Surface compatible with Windows 7 applications?

The answer is no and yes, depending on the version of the Surface. Don't expect Windows RT to work with traditional Windows 7 and Windows XP applications. The ARM processor won't run x86 applications. The x86-based Windows 8 version will run existing Windows 7 and XP applications.

6 Will Microsoft Office run on the Surface?

Office integration will be a key to the success of the Surface, and it will be a key differentiator between the Surface and the iPad or Google's Nexus 7. The Windows RT and Windows 8 versions of the Surface will run different versions of the Microsoft Office productivity suite. Microsoft has stated that the basic Office Home & Student 2012 RT

version will be included in the Windows RT version. This Office version includes Word, Excel, PowerPoint, and OneNote. Microsoft hasn't stated if Office will be included with the Windows 8 version, but it can run previous versions of the Office suite.

7 What are some of the differences between the Windows RT and Windows 8 Surface models?

The biggest difference is in the application support or lack of x86 application support in the Windows RT version. However, the Windows RT version will be thinner and lighter, weighing in at a mere 1.5 pounds compared to 2 pounds for the Windows 8 version. The Windows 8 version will also provide 1020p screen resolution, exceeding the Windows RT version's 720p resolution.

8 Will Microsoft be the only maker of the Surface?

Yes and no. Surface is a Microsoft brand, and only Microsoft will market that brand. However, other companies are sure to release similar tablets.

9 What's the price of the Surface?

At this point, Microsoft hasn't provided specific pricing for the Surface. However, it's clear that the Windows RT version and the Windows 8 version will have different audiences and hence different price points. The Windows RT version is targeted toward consumers and will presumably have a price point that's competitive with the iPad, which starts at $499. The Windows 8 version is targeted toward business professionals and will probably be priced closer to today's ultrabooks.

10 When is the Surface supposed to be available?

Microsoft has stated that it expects the consumer-oriented Windows RT version of the Surface to be available October 26, 2012. The Windows 8 version is expected a few months later, probably in the first quarter of 2013. ■

InstantDoc ID 143643

MATCH YOUR SERVER TO YOUR BUSINESS.

ONLY PAY FOR WHAT YOU NEED!

With a 1&1 Dynamic Cloud Server, you can change your server configuration in real time.

- Independently configure CPU, RAM, and storage
- Control costs with pay-per-configuration and hourly billing
- Up to 6 Cores, 24 GB RAM, 800 GB storage
- 2000 GB of traffic included free
- Parallels® Plesk Panel 11 for unlimited domains, reseller ready
- Up to 99 virtual machines with different configurations

LIFETIME DISCOUNT
1&1 DYNAMIC CLOUD SERVER

50% OFF*

INCLUDING CONFIGURATIONS, NO SETUP FEE
$24.99 per month (regularly $49.99 per month).

Parallels Plesk Panel

SUSE

OPTERON PROCESSOR AMD

- **NEW:** Monitor and manage your cloud server through 1&1 mobile apps for Android™ and iPhone®.

MEMBER OF united internet

www.1and1.com

1&1®

*Offer valid for a limited time only. Lifetime 50% off applies to base fee and configurations. Base configuration includes 1 processor core, 1 GB RAM, 100 GB Storage. Offer applies to new contracts only. 12 month minimum contract term. Other terms and conditions may apply. Visit www.1and1.com for full promotional offer details. Program and pricing specifications and availability subject to change without notice. 1&1 and the 1&1 logo are trademarks of 1&1 Internet, all other trademarks are the property of their respective owners.

Cloning Virtual Domain Controllers in Windows Server 2012

Quickly provide capacity and failover capability for your Active Directory forest

One benefit of virtualization is that because a virtual machine (VM) exists entirely in software, with no unique physical pieces, you should be able to copy (or *clone*) a VM and experience no loss in integrity. Cloning is a significant benefit of virtualization; you can quickly create new VMs without going through a tedious creation process every time. But can you clone a VM running any type of application? The answer to that question is, "It depends." This wishy-washy answer makes sense when you look at the contents of a VM in layers and see what is unique in those layers.

Sean Deuby

is technical director for *Windows IT Pro* and *SQL Server Pro* and former technical lead of Intel's core directory services team. He's been a directory services MVP since 2004.

Email

Twitter

Active Directory Was a No-Clone Zone

A VM's component virtual disks and configuration are designed to be cloned, but what about the base OS? That can be cloned, too, as long as it's not uniquely coupled to any physical components (such as a passthrough disk) and you resolve other potential conflicts such as the system's name and static IP address. A domain-joined VM presents another conflict, in that the machine's security identifier (SID) is the same as the original. There are a number of workarounds for this conflict—from the Sysprep process to the Sysinternals NewSID utility—that will generate a new SID for the cloned VM.

There are also application-level dependencies. In Active Directory Domain Service's (AD DS's) case, the major constraint against

cloning a VM is tied to the fact that each domain controller (DC) is an integral part of a larger whole, a distributed system of DCs. Even though a DC can easily be replaced if it fails, it's essential to keep the whole distributed system informed of each DC's status. Most of the time, the DC whose state has changed (e.g., has been recovered from a backup) notifies its replication partners. Relying on such self-checking has its drawbacks, however, and over time safeguards have been added so that if a DC detects certain behaviors with a replication partner—such as attempting to replicate attributes for an object that's already been deleted—it will reject all further updates.

If you trick a virtualized DC in Windows Server 2008 R2 or earlier by performing virtualization operations to it that it's not familiar with, bad things can happen. As a result of such mistakes, in the Windows Server 2012 product cycle, the AD team set a high priority for making AD safe to virtualize: They introduced the VM-GenerationID (VM Gen ID) into the hypervisor and built relevant logic into the OS and AD. My July column "Virtualization-Safe Active Directory in Windows Server 2012" goes into more detail about this solution.

Clones Equal Flexibility

But back to cloning. Making AD virtualization-safe in Server 2012 produced the side benefit of making it safe to clone AD. Cloning is an especially useful benefit for AD because it lets you quickly add capacity. Prior to Server 2012, the only way to add a DC to your AD forest was to create a new VM, then use Dcpromo to promote the VM to DC status. That method isn't such a big deal if you don't have a large AD forest with a correspondingly large ntds.dit directory database or if you have to only occasionally add or replace a DC—but if you're in a large or flexible environment, it really slows you down.

If you can rapidly deploy new DCs, you have a big edge in quickly recovering a domain or forest after a disaster, as I outlined in "How Windows Server 2012 Improves Active Directory Disaster Recovery." If you're building a private cloud, DC cloning lets you make the cloud

authentication and authorization infrastructure as elastic as the rest of its capabilities. If you need to quickly spin up a test environment or add capacity to a branch office, DC cloning will do it for you.

Of course, any new feature that affects the security infrastructure must come with appropriate administrative and security restrictions. You can't let just anyone create another DC. The challenge of any layered infrastructure is that whoever controls the lower layers can affect the upper layers. For example, the fastest SQL Server cluster in the world won't get much work done without network connectivity.

In a virtualized AD infrastructure, the hypervisor administrators have control over all VMs and therefore all virtual DCs (VDCs). It isn't possible to restrict which DC a hypervisor administrator tries to clone; therefore, the AD team built safeguards into the cloning process so that it works only if a VDC that's been authorized as a clone source was used.

Cloning Procedure

Before you can clone a Server 2012 VDC, both the server hosting the source VDC and the destination host must support VM Gen ID. Currently, only Windows Server 2012 Hyper-V supports VM Gen ID, but VMware and Citrix have the specification to incorporate it into their products. The PDC Emulator for the domain must also be running Server 2012 (but you can't clone it). Note that you can clone only a Server 2012 DC; you can't perform this operation on any earlier versions. And the fact that you have existing Server 2012 DCs means that you've already upgraded your forest and domain(s) to Server 2012, as I discussed in "Windows Server 2012 Simplifies Active Directory Upgrades and Deployments." The steps to clone a DC are as follows:

1. Grant a VDC permission to be cloned by adding it to the Cloneable Domain Controllers security group. You can use any AD management tool, such as Active Directory Administrative Center (ADAC), Active Directory Users and Computers (ADUC), or PowerShell via the Add-ADGroupMember cmdlet.

2. Use the Get-ADDCCloningExcludedApplicationList cmdlet to identify any programs or services running on the source VDC that might not be safely cloned.
3. Review the list, and add to the CustomDCCloneAllowList.xml file any programs or services that you believe will clone successfully (contact the vendor or conduct your own tests). This part of the process is another reason why DCs should be running a minimal number of applications and services. I'm not aware of any restrictions that would prevent cloning of a Server Core or Minimal Server Interface (MinShell) installation.
4. Run the New-ADDCCloneConfigFile cmdlet on the source VDC. This cmdlet is where you also specify new parameters for the cloned VDC, including name, IP address, subnet mask, DNS servers, and the AD site name it will be deployed to.
5. Shut down the source VDC and export it (and of course restart the host if it's intended to be up).
6. Import the clone into its destination host, and start it.
7. The Microsoft article "Active Directory Domain Services (AD DS) Virtualization" describes the cloning process and prerequisites in detail. Because you must run New-ADDCCloneConfigFile on the source VDC, shut it down, and export it whenever you want to clone a new DC, large shops that clone often might want to put the source VDC in its own site with no user subnets. This way, shutting down the VDC at a moment's notice won't have any production impact.

Universal Appeal

Cloning is another welcome feature in AD for Server 2012, whether you're in a large shop looking to quickly add capacity, a midsized organization needing to provide failover to branch offices, or a small business using VDC cloning for AD disaster recovery. ■

InstantDoc ID 143948

FAQ

Answers to Your Questions

Q: How can I make sure my Deleted Items folder is empty in Microsoft Outlook?

Jan De Clercq

William Lefkovics

John Savill

A: I had a user the other day who insisted his Deleted Items folder was empty, but his mailbox was still pushing against the company's mailbox size limit policy. I've seen users accidentally move content to unexpected places without realizing it. For example, in Outlook it's possible to drag and drop a mail folder into the Calendar, Contacts, Tasks, or even Notes folders. Or the content could still be in Deleted Items, even if it doesn't appear to be so to the user.

The person who assured me his Deleted Items folder was empty was actually selecting the Deleted Items folder in the Navigation pane, highlighting the content in the main pane, then deleting the highlighted content. This method works, although it's somewhat tedious, but it misses content that might have been deleted from within subfolders. When you delete a folder, its contents are moved to Deleted Items as a subfolder. The contents of the subfolder aren't visible in Deleted Items unless the subfolder is selected in the Navigation pane. Also, when you select Deleted Items, it doesn't show the folders in the main pane; you have to click the little plus symbol or arrow beside Deleted Items in the Navigation pane for those folders to appear, as Figure 1 shows.

To delete these folders, you have to either do so one at a time, manually (not a good idea), or use the more logical Empty "Deleted Items" Folder or Empty Folder option from the right-click menu on the Deleted Items folder. You can also use the Empty Folder button on the Folder tab of the Ribbon in Outlook 2010 or go to Tools, Empty "Deleted Items" Folder in Outlook 2007 or Outlook 2003.

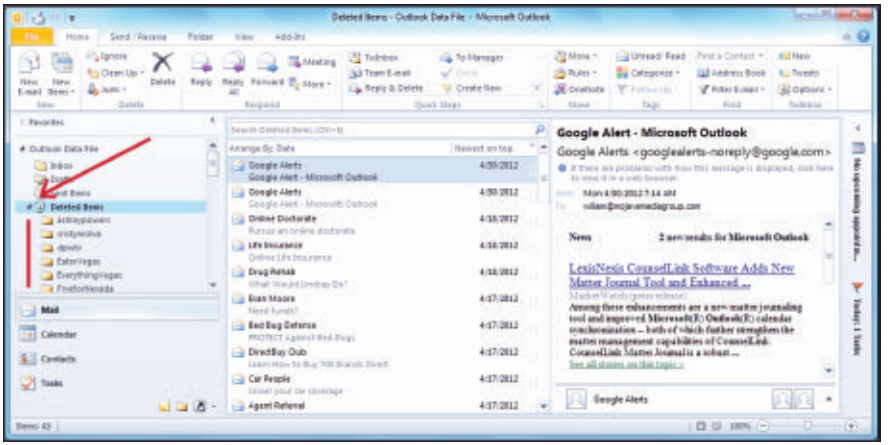


Figure 1
Expanding Deleted Items in Outlook to Show Deleted Subfolders

In addition, Outlook makes it easy to view the size of folders within the hierarchy so that you can identify where the greatest mailbox volume resides. You can right-click the account in the Navigation pane and select Data File Properties (or Properties) from the bottom of the context menu. On the General tab of the Properties dialog box, click the button for Folder Size to open a window listing individual mailbox folder sizes in kilobytes. Figure 2 shows an example with a small amount residing in Deleted Items. Unfortunately, this window isn't resizable, so if you have many folders, you'll have to scroll through them to see the full list.

Although the user I was working with claimed the Deleted Items folder was emptied, I was able to use this method to find a large amount of content still in that folder. Exchange administrators can also access this information without using the Outlook client, of course, by using Exchange Management Shell (EMS) and the Get-MailboxFolderStatistics cmdlet.

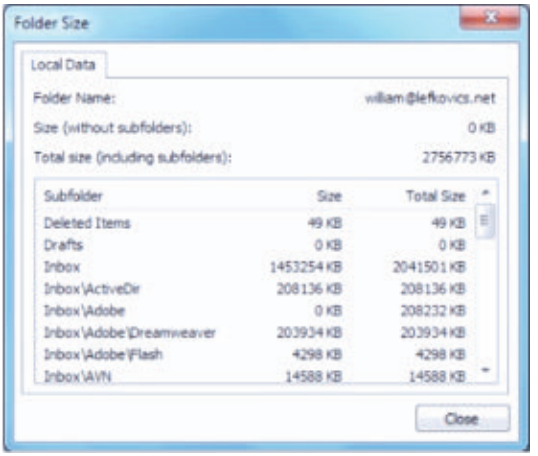


Figure 2
Viewing Actual Folder Sizes in Microsoft Outlook

—William Lefkovics

InstantDoc ID 143954

Q: Does BitLocker Drive Encryption support a recovery method that calls on Active Directory for storing the recovery information?

A: Yes, BitLocker Drive Encryption (BDE) supports a recovery method whereby the recovery password is automatically stored in Active Directory (AD). The BDE recovery password is a 48-bit numerical key that's generated during BitLocker setup. You can save it to a file or print it, or it can be automatically saved in AD.

To automatically store recovery passwords in AD, make sure that all computers can connect to AD when they enable BitLocker. Storage of BDE recovery information in AD is based on an AD schema extension that creates extra attributes to attach BDE recovery information to AD computer objects. Windows Server 2008 and Windows Server 2008 R2 domain controllers (DCs) include this extension by default. On Windows Server 2003, you must install the BitLocker-specific schema extension, which you can download from the "BitLocker Deployment Sample Resources" page on the MSDN website.

To facilitate the viewing and retrieving of the BDE recovery passwords from AD, Microsoft provides a Microsoft Management Console (MMC) Active Directory Users and Computers snap-in extension. It adds a BitLocker Recovery tab to the properties of the AD computer object that shows all BDE recovery passwords associated with a particular computer. For Windows Server 2008 R2, the BitLocker Active Directory Recovery Password Viewer tool is an optional feature included in the Remote Server Administration Tools (RSAT). For Server 2008, RSAT can be downloaded from the Microsoft Download Center. For more information about this topic, you can also read the Microsoft article "Configuring Active Directory to Back up Windows BitLocker Drive Encryption and Trusted Platform Module Recovery Information."

—Jan De Clercq

InstantDoc ID 143832

Q: Will Windows Server 2012 let you shrink and expand virtual hard disks while online?

A: Windows Server 2012 introduces the ability to merge snapshots for virtual hard disks (VHDs) while they are online, in addition to the ability to set the parent VHD and mirror operations. However, the ability to shrink, expand, compact, and convert a VHD isn't possible while the VHD is online. Any virtual machine (VM) using the VHD will need to be stopped before you attempt these operations.

—John Savill

InstantDoc ID 143383

Q: What is VM Generation ID in Windows Server 2012 Hyper-V?

A: VM Generation ID is a new virtual machine (VM) attribute in Windows Server 2012 Hyper-V that's used to enable specific applications running in a VM to detect if something has happened to the VM to affect its "place in time."

As an example, look at a domain controller (DC), the key service that uses the VM Generation ID (at the time this FAQ was written). Taking a snapshot of a DC VM then applying that snapshot later on is a very bad practice, because it moves that DC back in time. This results in identifiers being reused, causing security and replication problems (this stems from the fact that the DC has no idea that a snapshot was applied).

With the VM Generation ID, any time an operation on the VM occurs that changes that VM's place in time (moving it backwards), then Hyper-V will change the VM Generation ID of the VM. Such an operation could include a snapshot being applied, a VM being imported, or a restore occurring from a backup of the VM, and more.

The change in the VM Generation ID allows services to constantly compare their cached value of VM Generation ID (ms-DS-Generation-Id

for Active Directory—AD) to the actual VM Generation ID of the VM. If they don't match, the service knows something has happened to the VM's place in time and can react accordingly. In the case of DCs, if the VM Generation ID changes, then the DC will invalidate its RID pool and changes to invocation ID for the AD database (such as the database identifier), which stops duplicate security ID objects from being created and ensures proper replication.

—John Savill

InstantDoc ID 143593

Q: Can I use a workflow for application deployment from System Center 2012?

A: System Center Configuration Manager 2012 features a great web-based software catalog for enterprises that lets users request software by using a web browser. Microsoft has released a solution accelerator called the Microsoft Application Approval Workflow (AAW), which works with System Center Configuration Manager, System Center Service Manager, and System Center Orchestrator to provide a rich workflow, including authorization for user application requests.

The accelerator is available for download at Microsoft's Application Approval Workflow website and includes detailed deployment documentation. Its key features offer you the ability to do the following:

- Synchronize Configuration Manager applications data into the Service Manager database
- Monitor and transport Configuration Manager Application Catalog requests requiring approval to Service Manager and open a service request
- Return the completed approval workflow status to Configuration Manager for handling
- Let administrators define and maintain application selection criteria for specific applications or application groups and specific users or user groups

- Track application approval service requests and view application catalog contents in Service Manager

Essentially, users continue to use the Configuration Manager web portal for application requests; however, those requests are then converted to Service Manager requests, which can then be approved and processed before ultimately being acted upon by Configuration Manager. Behind the scenes, Orchestrator performs monitoring and acts on the requests.

—John Savill

InstantDoc ID 143737

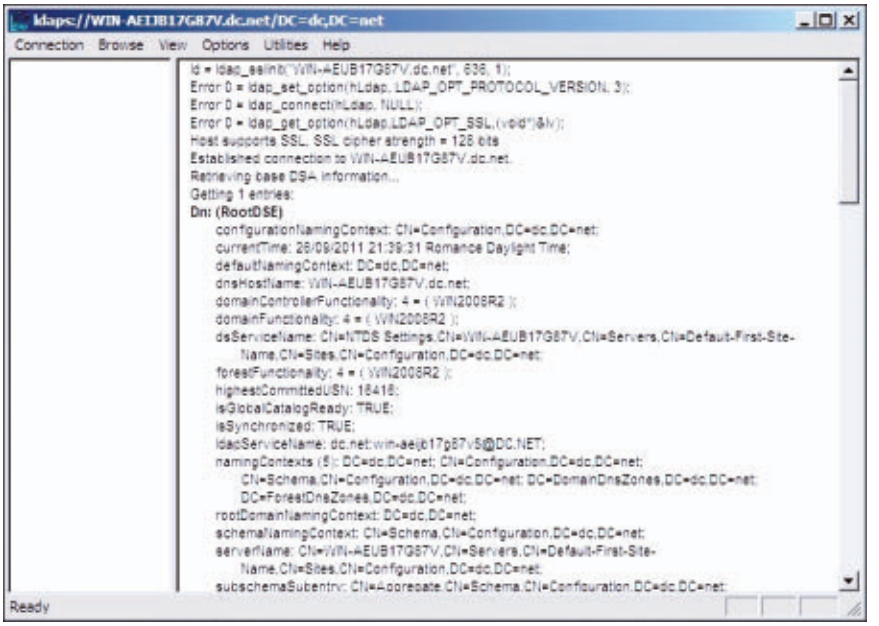
Q: How can I easily verify LDAP over SSL connectivity to my Windows DCs?

A: To verify that LDAP over SSL (LDAPS) connectivity is operational and configured correctly on your domain controllers (DCs), you can use the LDP tool. LDP is installed by default on a Windows Server 2008 DC. On Server 2008 member servers and Windows 7 or Windows Vista machines, you must install the Remote Server Administration Tools (RSAT) to get access to LDP.

To open LDP, click Start and type ldp in the Search box. Click the LDP Connection menu option, then click Connect. In the Server field, type the Fully Qualified Domain Name (FQDN) of the DC to which you want to connect. Ensure that the port is set to 636 (this is the default LDAPS port), the Connectionless check box is cleared, and the SSL check box is selected, then click OK. If LDAPS is configured properly, the LDP command output should display "Host supports SSL," as Figure 3 shows.

Next, click the Connection menu option again, select Bind, and click OK. If LDAPS is configured properly, the LDP command output should display the user name and domain name that you used for authenticating with LDP to Active Directory (AD). For troubleshooting

Figure 3
LDP Tool Showing Correctly Configured LDAPS



LDAPS connectivity, I advise you to read the Microsoft article "How to troubleshoot LDAP over SSL connection problems."

—Jan De Clercq

InstantDoc ID 143831

Q: I disabled hibernation on Windows 8—so why does startup seem to take longer?

A: Windows 8 introduces a fast, new startup capability, which, because of several improvements, allows it to start quicker than an equivalent Windows 7 system. One of the changes is that the kernel session is saved to disk (which includes device and system service state) when the machine is shut down, then read at system startup instead of reinitializing all system components and drivers.

This speeds up shutdown and startup, saving a lot of time. The kernel session is saved in the hibernation file (the same place used if a full system hibernation of a running system is saved). If you disable

the hibernation file using the following command (from an elevated command prompt):

```
powercfg /h off
```

then the hiberfil.sys is removed, and there's no place to store the kernel session. This means the fast startup process from a saved kernel session isn't possible.

You need to fix it by re-enabling hibernation, to enable Windows to create a new hiberfil.sys and allow the saving and restoring of the kernel session. To do so, use this command:

```
powercfg /h on
```

■

—John Savill

InstantDoc ID 143523

Introducing Windows Server 2012

Get the scoop on this feature-rich release

By Michael Otey and Sean Deuby

Microsoft's most significant server OS release since Windows 2000 has finally arrived. By the time you read this article, Windows Server 2012 should be available for download or purchase. The *Windows IT Pro* technical team has been playing with this OS for about a year, and it's a feature-packed beast. (I still believe Win2K was a more significant release than Server 2012, simply because the former established Microsoft's position as a credible enterprise server vendor.) The Server 2012 reviewer's guide has more than 200 pages describing new or improved features—and those are just the most significant ones.

Adding to the anticipation of this release is the fact that all features in

Server 2012 will be available in both the Standard and Datacenter editions. This is a windfall for small-to-midsized businesses (SMBs), which have traditionally been left at the door when features that they needed, such as DFS Replication (DFSR), were available only in Enterprise or Datacenter OS editions.

The licensing model also contains fewer editions. Server 2012 basically has three editions. Essentials is designed for small business environments. Standard, which has only two virtual-instance licenses, is for low-density or nonvirtualized environments. Datacenter is by far the most expensive but has unlimited virtual instances. Your decision about which edition to purchase depends on your plans for virtualization. There's also an OEM-only Foundation edition that provides a basic network infrastructure—Active Directory (AD), remote access, and file and print sharing.

I would add one more product to this list of editions: Microsoft Hyper-V Server 2012, which *Windows IT Pro* reviewed in the June 2012 issue. Though not a full OS, Hyper-V Server 2012 is one building block that you should consider when determining which Server 2012 edition you need. For more information about the various Server 2012 versions and how they differ, take a look at John Savill's FAQ "What are the versions of Windows Server 2012 and how do they differ?"

Storage

Although the new and improved Hyper-V capabilities have been getting the most press, I'd argue that there are actually more improvements to the storage platform than to the hypervisor. And some of these improvements—for example, Live Storage Migration—enable cool Hyper-V capabilities such as Shared Nothing Live Migration. Let's look at how businesses of different sizes might take advantage of these new capabilities.

Small business. Small businesses have typically been at the back of the line when Microsoft hands out new OS features. After years of focusing on the high end—which it continues to do with its cloud

Michael Otey

is senior technical director for *Windows IT Pro* and *SQL Server Pro* and author of *Microsoft SQL Server 2008 High Availability with Clustering & Database Mirroring* (McGraw-Hill).

Sean Deuby

is technical director for *Windows IT Pro* and *SQL Server Pro* and former technical lead of Intel's core directory services team. He's been a directory services MVP since 2004.

computing focus—the company has added a nice storage feature for small businesses: Storage Spaces.

Every growing small business faces the challenge of how to increase its storage and availability in a linear, cost-effective manner. At the low end, inexpensive DAS inside a server provides a moderate amount of storage at a reasonable price. To expand application-oriented storage beyond what you can cram inside a server, however, you need an external storage array, typically a SAN. You must also use an external array if you want high availability for an application or virtualization host. The problem is that a storage array that gives you the options you need (plus some future flexibility) is easily going to cost something in the five-figure range. That's quite an investment for a small company.

Storage Spaces is designed to fill this gap between DAS and SAN, by providing storage virtualization based on inexpensive Serial ATA (SATA) and Serial Attached SCSI (SAS) disks, in inexpensive configurations. You can take a collection of disks in a Just a Bunch of Disks (JBOD) array (i.e., a configuration with no special RAID capabilities); configure them with Storage Spaces to create virtual disks with spanning, mirroring, or parity; and create volumes from them. And because the Storage Spaces subsystem operates at a lower layer than the OS's disk management layer, all volumes that Storage Spaces create appear as regular volumes to Disk Manager and all applications. This architecture also lets you create Cluster Shared Volumes (and therefore clusters) from JBOD arrays. Published numbers from Microsoft show that disk I/O performance with Storage Spaces is within a few percentage points of native speeds.

There are actually more improvements to the storage platform than to the hypervisor.

Instead of building this arrangement on premises, what about using Software as a Service (SaaS) and Infrastructure as a Service (IaaS) and having little or no on-premises infrastructure? It's definitely an option, but Storages Spaces provides such an inexpensive means for adding and managing capacity and high availability that I think it provides a strong case for remaining on premises for a while.

Another Server 2012 storage feature benefits not just small businesses, but all business: data deduplication. Dedupe, as it's known to IT pros who like to shorten long terms, is a technology that compares stored data at the block level. When it encounters duplicate blocks of data, deduplication replaces the duplicate block with a simple pointer to the reference block, saving space. When enabled, the deduplication process runs as a low-priority background process, and Microsoft predicts savings of anywhere from 2:1 for file shares to 20:1 for virtual disk storage. I saw a demonstration using data dedupe against a 2TB USB drive used to store Virtual Hard Disk (VHD) files, with 95-percent space savings. There isn't much benefit trying to dedupe active virtual disk volumes because they're changing. But you'll get huge benefit out of deduping virtual machine (VM) libraries.

Midmarket. An important Server 2012 capability is the ability to upgrade the file server role, referred to in Microsoft documentation as the Server Message Block (SMB) file server, from its traditional use of simply storing user data at a file level to storing application data at a block level. This change means that you can use Server 2012 file servers not only for user files but also as remote virtual disk storage for Microsoft Hyper-V and SQL Server, as well as for VMware vSphere (through its NFSv3 and NFSv4.1 support). This capability opens up many options for your virtual disk storage and is a key component of Hyper-V Live Storage Migration.

Windows Server 2012 is a feature-packed beast.

Enterprise. Improvements abound for the enterprise customer. Clusters now scale out to 64 nodes, with as many as 4,000 VMs in a single cluster, thanks to Cluster Shared Volumes version 2. And the enhancements to the file server role that I described let you create highly available, scalable storage for Hyper-V and SQL Server clusters, using SMB file server clustering—yes, with file servers! You can even use a relatively inexpensive file server cluster as a front end for an expensive Fibre Channel SAN. Doing so lets you scale up the SAN without changing its (expensive) attachments to the rest of the network. I haven't run across performance numbers, but Microsoft has

gone to great pains with SMB 3.0 to provide both performance and fault tolerance.

This is a very short list of the many storage improvements in Server 2012, but I wanted to mention one more item. The new OS brings great improvement to a humble yet crucial storage component: Chkdsk. In what I think of as a blinding flash of the obvious, Chkdsk now runs in two phases. The first phase runs online, scanning a volume for errors and flagging them. The second phase runs on reboot and simply corrects the errors. This design change ties Chkdsk repair time to the number of errors on the volume, not the size of the volume. As a result, boot-time Chkdsk error correction on large volumes that used to take many hours now takes only minutes!

Management

The biggest changes around management of Server 2012 can be grouped into two areas: Server Manager and Windows PowerShell. Server Manager has been around since Windows Server 2003, and PowerShell has been around since Windows Server 2008. Both evolutions have been a microcosm of many other technologies that Microsoft has pointed at IT pros. Both started small, and both were soundly ignored and pushed out of the way by the vast majority of systems administrators. (Did anyone *not* check the *Do not show this next time* check box for Windows Server 2003 Server Manager?) But as each technology grew in capability—and, let's be honest, they were increasingly difficult to work around—we began to use them more often. Both are now central to server management in Server 2012.

Server Manager (which Figure 1 shows) is where you manage all role-related functions and many (but not all) local server management and OS functions. You manage the installed roles in the left pane, add and remove roles on the Manage menu, and perform general management functions on the Tools menu (which is expanded in the figure). One key aspect in this version of Server Manager separates it from previous versions: It's designed to manage multiple servers, or

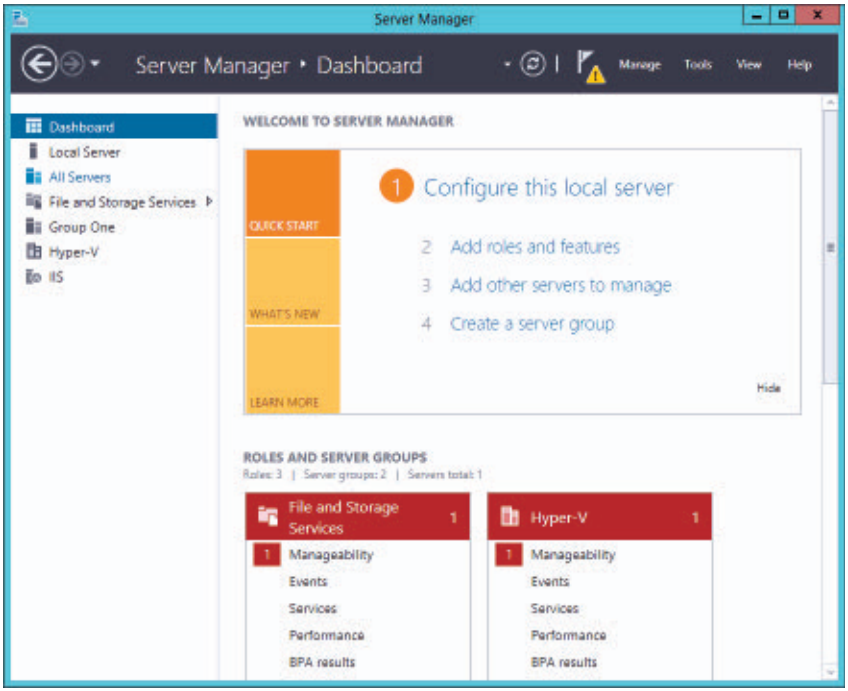


Figure 1
Server 2012 Server Manager

a server role across multiple servers, from one console. See "Getting Around in Windows Server 2012, Part 2: Server Manager" for tips on using Server Manager.

PowerShell pretty much does it all in Server 2012. In Windows Server 2008 R2, PowerShell consists of 456 cmdlets in 10 modules. In Server 2012, PowerShell has more than 2,300 cmdlets in 239 modules—over five times its predecessor. Although that's a lot of cmdlets to keep track of, it's also much closer to a 1:1 ratio of cmdlet to task. In other words, instead of needing to string several cmdlets together to accomplish a task, you can probably get the job done with one Server 2012 PowerShell cmdlet. With earlier releases, PowerShell support was limited. Previously, you typically needed to use either Windows Shell scripting or VBScript to accomplish many common tasks. The extended PowerShell support promises to eliminate this issue. Further, the new PowerShell Integrated Scripting Environment (ISE) has features such as IntelliSense that help you build scripts more easily.

Every new management console is a shell that runs PowerShell, and you can extract the PowerShell code from many of them to reuse or modify. Active Directory Administrative Center, for example, has a PowerShell history viewer that shows you the underlying PowerShell cmdlets that are used for every GUI task that you execute.

PowerShell adoption remains slow with IT pros, however. Judging from recent experience, I'd say no more than 20 percent of systems administrators are actively using this scripting technology. This will slowly change, as PowerShell continues to supplant other forms of administrative automation.

Hyper-V

Arguably, the biggest changes in Server 2012 are found in its improved support for virtualization with Server 2012 Hyper-V. Server 2012 Hyper-V has essentially pulled Microsoft even with (or in some cases ahead of) the virtualization capabilities found in the vSphere platform. Let's dive into some of the important Server 2012 Hyper-V enhancements, beginning with scalability.

Scalability. Raw scalability has long been one of the areas in which vSphere has held a significant edge over Hyper-V. The Server 2012 release changes all that. Server 2012 Hyper-V boasts huge improvements in scalability over the previous version. Table 1 highlights some of the most significant scalability improvements.

You can see that host scalability has jumped tremendously, with the Server 2012 Hyper-V host now able to support as many as 320 logical processors and 4TB of RAM. This improvement enables far higher levels of server consolidation with Hyper-V than ever before and exceeds the total scalability in vSphere 5. Likewise, Server 2012 Hyper-V supports much more scalable guest VMs. Windows Sever 2008 R2 had a pretty tight cap on VMs, allowing only 4 virtual CPUs (vCPUs). That limit wasn't enough for many workload-intensive systems, such as SQL Server databases, which can be more demanding. The new Hyper-V now supports as many as 64 vCPUs and guests with up to 1TB of

Table 1: Windows Server 2012 Hyper-V Improved Scalability

System	Resource	Windows Server 2008 R2 Hyper-V	Windows Server 2012 RC Hyper-V	VMware vSphere 5 Enterprise Plus
Host	Logical processors	64	320	160
	Physical memory	1TB	4TB	2TB
	Virtual CPUs per host	512	2048	2048
VM	Virtual CPUs per VM	4	64	32
	Memory per VM	64GB	1TB	1TB
	Active VMs per host	384	1024	512
	Guest NUMA	No	Yes	Yes
Cluster	Maximum nodes	16	64	32
	Maximum VMs	1000	4000	3000

RAM—enough for almost all workloads. Again, you can see that Server 2012 Hyper-V actually exceeds the 32 vCPUs that vSphere allows. Just as important for overall performance is support for guest non-uniform memory access (NUMA). Guest NUMA allows the physical RAM in the host to be aligned to the VM processors, reducing the need to perform memory page lookups and thereby significantly improving VM performance.

Although not technically a part of the virtualization stack, the clustering in Server 2012 has been significantly enhanced as well. Previous versions of Windows Server were limited to 16-node clusters. Server 2012 has blown the roof off that limit by allowing clusters with as many as 64 nodes supporting as many as 4,000 VMs. This lays the foundation for the dynamic data center by vastly expanding the ability to move VMs between hosts, including hosts that are in different geographic locations.

Live migration and Live Storage Migration. Live migration refers to the ability to move running VMs between Hyper-V hosts, whereas Live Storage Migration refers to the ability to move VM storage

artifacts, such as VHD files, between Hyper-V hosts, with no downtime. Hyper-V live migration was first introduced with Server 2008 R2. Although it provided a good start, that version of Hyper-V lacked the ability to perform multiple, simultaneous live migrations, leaving it short of what VMware could do. Server 2008 R2 was incapable of Live Storage Migration but did have an option for Quick Storage Migration. (In earlier Hyper-V terminology, *quick* was a euphemism for the fact that downtime would still occur.) vSphere had VMware Storage vMotion technology, so this was another area in which Hyper-V was playing catch-up. Server 2012 Hyper-V adds the ability to perform Live Storage Migration between Hyper-V hosts, with no VM downtime. With Live Storage Migration, the VHD and configuration files are copied from the source system to the destination storage. All write operations are then mirrored to both the source and destination storage devices. After the source and destination storage locations are in sync, VM access to the VHD and VM files is transferred to the destination, and the source files are deleted. (Live Storage Migration moves a VM's files, not the VM itself.)

Server 2012 Hyper-V supports not only multiple concurrent live migrations but also multiple concurrent Live Storage Migrations. That support essentially brings Windows Server's Hyper-V on par with vSphere 5. In addition, by building on top of the new SMB 3.0 enhancements, Server 2012 Hyper-V supports live migration and Live Storage Migration without the need for a cluster or shared storage. This capability is sometimes referred to as Shared Nothing Live Migration. This migration works in a couple of ways. Server 2012 Hyper-V provides the ability to perform live migrations when the VMs are stored on a network file share, plus you can perform live migrations directly between Hyper-V hosts.

Hyper-V Replica. Live migration protects against planned downtime by letting you move VMs to other hosts and then perform maintenance on the Hyper-V host, with no end-user disruption. Hyper-V Replica technology is included as a part of Server 2012 and can replicate

VMs to provide improved business continuity and disaster recovery. Hyper-V Replica asynchronously replicates VMs between hosts and offsite locations and provides failover if a failure occurs in the primary site. Hyper-V Replica can replicate one or more VMs on the Hyper-V host. It doesn't require a SAN or other shared storage solution, making Hyper-V Replica a cost-effective disaster recovery solution.

Hyper-V Replica works between two Windows Server systems, each of which must have Server 2012 and the Hyper-V role installed. Hyper-V Replica works in both clustered and unclustered environments. Replication works in one direction, so if you want to recover automatically back to the primary site, then both ends should be configured as replica servers. Before replication can start, you need to make an initial copy of the VHD of the VMs that you want to replicate. You can enable Hyper-V Replica by using either PowerShell or Hyper-V Manager. Using Hyper-V Manager, right-click the Hyper-V server that you want to act as a replica server, then select the new *Replication Configuration Enabled as a Replica server* option, which you can see in Figure 2.

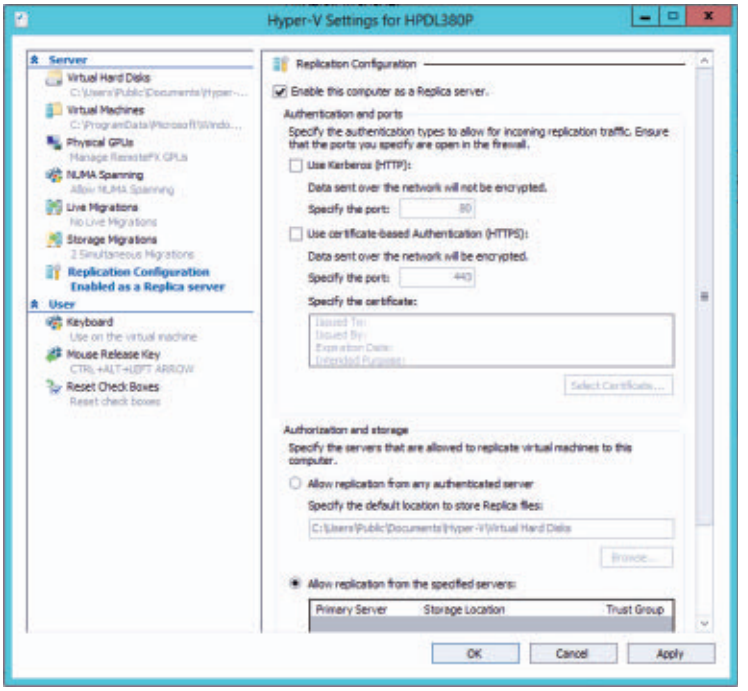


Figure 2
Enabling Hyper-V Replica

The Replication Configuration settings let you enable the Hyper-V server to act as a replica server. You select the authentication method that will be used to connect to the replication target, as well as the authorization and storage that will be used. After you enable replication at the Hyper-V server level, you can specify the VM that will be replicated by right-clicking the VM in Hyper-V Manager and then selecting the Enable Replication option, which in turn runs the

Enable Replication Wizard. The Enable Replication Wizard lets you indicate the VHDs that will be replicated, set up the recovery history (which basically instructs the replicated VM to perform snapshots for point-in-time recovery), and choose the initial replication method.

Extensible Virtual Switch. To better support multitenancy and to allow more flexible enterprise deployments, Server 2012 Hyper-V provides an all new Extensible Virtual Switch. The Extensible Virtual Switch provides tenant isolation and traffic shaping, as well as enabling third parties to develop custom plug-ins for it. Earlier versions of Hyper-V supported internal, external, and private networks. The Extensible Virtual Switch provides a much greater degree of flexibility. You can create multiple virtual switches and you can create and connect multiple virtual network adapters to those switches. (Each virtual switch can be connected to only one physical network adapter.) The Extensible Virtual Switch supports three types of third-party extensions:

- capturing extensions, which allow the Extensible Virtual Switch to capture and monitor network traffic but don't allow any modification of network traffic
- filtering extensions, which allow the Extensible Virtual Switch to capture, inspect, and optionally drop network packets
- forwarding extensions, which allow the Extensible Virtual Switch to modify the routing information in network packets

More Hyper-V enhancements. There are so many improvements in Server 2012 Hyper-V that I can't cover them all in one article. In addition to the major enhancements already discussed, there are many other important enhancements:

- Resource metering—Server 2012 Hyper-V adds the ability to track how virtual resources are being used. Resource-consumption information can be used for chargeback or to plan for the internal allocation of private cloud resources. Collected metrics include average CPU usage per VM, average memory usage per VM, maximum memory usage per VM, and total incoming and outgoing network traffic.

- Hyper-V module for PowerShell—The Hyper-V module for PowerShell lets you perform all the Hyper-V management tasks from PowerShell. This module includes more than 160 cmdlets, allowing you to manage Hyper-V servers, VMs, and VHDs.
- Virtual Fibre Channel—New Virtual Fibre Channel support lets you connect VMs directly to Fibre Channel storage. The Virtual Fibre Channel virtualizes host bus adapter (HBA) ports in the Hyper-V host and exposes them to the guest VMs. You can assign as many as four Virtual Fibre Channel adapters per VM.
- New VHDX disk format—Server 2012 Hyper-V adds a new VHD format called VHDX, which supports as much as 64TB of storage. Previously, Hyper-V VHDs were limited to 16GB. The new VHDX format also provides protection from corruption that stems from power failures and prevents performance degradation on some large-sector physical disks.
- Single root I/O virtualization (SR-IOV)—SR-IOV lets you assign a physical network adapter that supports SR-IOV directly to a VM. Providing a VM with direct connectivity to a physical network adapter can maximize the network performance that's available to the VM.
- Microsoft RemoteFX—First introduced with Server 2008 R2, RemoteFX allows advanced graphics to be rendered on the Hyper-V host and delivered to the client via RDP. Server 2012 Hyper-V enables the use of multiple host graphics processing units (GPUs) and software-based GPUs. Multiple VMs can share a GPU on the host.

For a quick overview of the different Server 2012 Hyper-V components, you might want to check out Microsoft's Windows Server 2012 Hyper-V Component Architecture poster.

Windows Server 2012 Networking

Networking is one of those IT infrastructure underpinnings that doesn't always get a lot of attention but that's vital for implementing

Networking is especially important in today's connected public and private cloud scenarios.

many higher-order capabilities, such as file sharing, application serving, virtualization, and the cloud. Networking is especially important in today's connected public and private cloud scenarios. Server 2012 has several important new networking features and enhancements.

Built-in NIC teaming. Although there are many networking enhancements in Server 2012, one of the most important is support for built-in NIC teaming. NIC teaming allows multiple network adapters to work together as a unit so that they can provide protection against failure, as well as improved network performance. NIC teaming was built into vSphere; earlier versions of Windows Server had limited support for NIC teaming, restricting it to specialized network adapters from specific vendors. Plus, Microsoft wasn't completely behind this earlier NIC teaming implementation. If you ran into network problems, one of the first things Microsoft support would have you do was to turn off NIC teaming. With Server 2012, Microsoft fully supports the feature—and even better, the feature works across multiple network adapters from different vendors.

To create a new NIC team, you use Server Manager to create a new management group that includes the Server 2012 system on which you want to create the NIC team. To configure NIC teaming, right-click a server in the group and select Configure NIC Teaming from the context menu. Then from the Teams pane, select New Task. This will display the *New team* window, which you can see in Figure 3. To create a new NIC team, provide the NIC team with a name and then select the network adaptors that will be included in the NIC team. Do so by selecting the check boxes to the left of the desired network adapters.

DNS security. DNS Security Extensions (DNSSEC) is a set of extensions to the DNS protocol. These extensions add a level of security to the DNS information that's stored on the servers. DNSSEC was first added to Server 2008 R2; Server 2012 enhances the DNSSEC implementation. Some major improvements in this OS include support for dynamic updates in DNSSEC signed zones, support for updated DNSSEC standards such as NSEC3 and RSA/Secure Hash

Algorithm-2 (SHA-2), and automated trust-anchor distribution using AD. DNSSEC is configured by using either PowerShell or the updated DNS Manager.

Quality of Service. Server 2008 R2 supported a limited Quality of Service (QoS) implementation that let you control the maximum bandwidth used. Server 2012 expands the reach of QoS by adding the ability to set a minimum bandwidth. Although the previous maximum could prevent a given service or application from consuming all the available bandwidth, it couldn't truly ensure that there would be adequate network bandwidth for other applications. That's exactly what the new minimum bandwidth settings allow. When network bandwidth is available, each service can take as much bandwidth as it needs. However, when the network is congested, the new minimum bandwidth setting makes sure that capacity is reserved for each service so that all services can consume only their share. This lets you better meet service level agreements (SLAs) by ensuring that each service always has a given amount of network bandwidth available. Server 2012 enforces minimum bandwidths by using the new network packet scheduler or by using network adapters that provide support for Data Center Bridging (DCB). The network scheduler is preferable when many traffic flows require minimum bandwidth levels. The DCB method is preferable for few traffic flows, iSCSI traffic, or other traffic that originates outside the server.

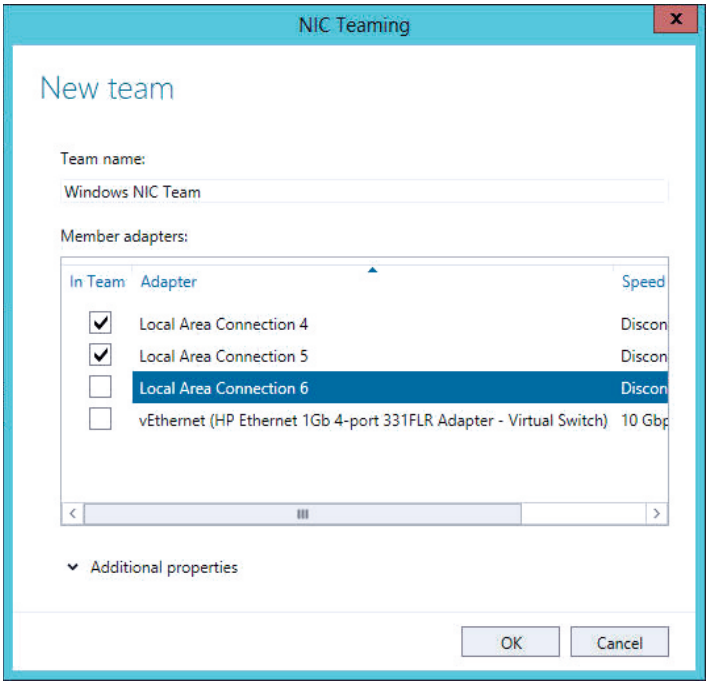


Figure 3
Configuring NIC Teaming

iSCSI target and diskless network boot from iSCSI. One feature that comes to Server 2012 from Windows Storage Server is the ability to act

Windows Server 2012 is quite possibly the most important release of Windows Server since Windows 2000.

as an iSCSI target. The iSCSI target capability essentially allows Server 2012 to act as an iSCSI SAN. Although this capability is no replacement for a full-blown iSCSI SAN, it can be a handy addition for SMBs looking to augment their storage capabilities or to improve their availability by using technologies such as failover clustering and live migration.

Closely related is the ability to boot from an iSCSI target. This capability lets you boot networked systems from centrally stored VHD images. Doing so can make central management of images easier and lets you save disk space by booting multiple systems from differencing disks that are built from the same shared image.

Dynamic Host Configuration Protocol server failover. Dynamic Host Configuration Protocol (DHCP) servers can be a single point of failure on a network because of the critical nature of the service that they provide. If the DHCP server is unavailable, then the network client can't obtain new IP addresses to connect to network resources. Server 2012 adds support for the new DHCP Failover protocol, which lets DHCP servers fail over without the need for failover clustering. The DHCP Failover protocol allows two DHCP servers to synchronize their IP address leases; if one of the servers becomes unavailable, the other assumes the job of handing out addresses for the subnet. You can also use the protocol to set up load balancing between the two DHCP servers.

Other networking enhancements. Server 2012 includes a host of other important networking improvements:

- Microsoft IIS CPU throttling—This feature lets you set limits on the amount of CPU resources that a given website can consume.
- WebSockets—Support for WebSockets is added to Internet Information Services (IIS) 8 in Server 2012. WebSockets is an open industry standard protocol that allows web servers to push messages to a client rather than waiting for the client to make requests from the server.
- Dynamic IP Restrictions—A new IIS 8 improvement, Dynamic IP Restrictions lets you set up filters in Server 2012 to dynamically block server access for IP addresses that exceed a specified

number of requests within a given time. You can also configure the response that the server gives when a specific address is blocked.

- FTP logon attempt restrictions—Another IIS 8 improvement, FTP logon attempt restrictions let you block access to the FTP server for a given time period following invalid logon attempts.
- Improved DirectAccess—First introduced with Server 2008 R2, DirectAccess provides an always-on alternative to remote VPN access. Server 2012 makes it much easier to deploy DirectAccess. In addition, the feature can coexist with VPN implementations and can be installed on Server Core.
- Enhanced BranchCache—Also a part of Server 2008 R2, BranchCache improves the file server performance of a remote site by allowing the site to locally cache requested content. Server 2012 brings several improvements to BranchCache, including the ability to deduplicate and encrypt the cached data.

Take a Look

Server 2012 is quite possibly the most important release of Windows Server since Win2K. Server 2012 fully embraces the goals of scripted multiserver management while enhancing the built-in Hyper-V virtualization support to equal or exceed the standards set by vSphere. Server 2012 promises to transform the way that businesses manage their Windows IT infrastructure. You can check it out for yourself by downloading the Windows Server 2012 Release Candidate. ■

InstantDoc ID 143995

Microsoft Releases Windows Server 2012

Improvements in storage, virtualization, and management are worth a look

Windows Server 2012, arguably the most significant server release Microsoft has ever offered, became available for evaluation and purchase to customers around the world on September 4, 2012. Server 2012 offers a simplified licensing model that includes all features of the OS in all editions of Server. You'll find improved management capabilities in Server Manager and PowerShell. Storage improvements are numerous, and Hyper-V enhancements include scalability, live migration upgrades, and storage live migration capabilities. *Windows IT Pro* brings you ongoing coverage of Server 2012, with in-depth treatment of significant features, breaking news, and analysis. Visit our Windows Server 2012 page for the latest news and technical features. ■

InstantDoc ID 143935

Top 10 Windows Server 2012 FAQs

1. How do I enable and view the Windows Server 2012 Hyper-V metric information?
2. What is the difference between installing Windows Server 2012 as Server Core or server with a GUI?
3. How many processors are supported on supported Linux virtual machines with Windows Server 2012?
4. Will Windows Server 2012 let you shrink and expand virtual hard disks (VHDs) while online?
5. What are the new Hyper-V limits with Windows Server 2012 Release Candidate?
6. Is the Windows Server 2012 data deduplication feature also available in Windows 8 client?
7. I have virtual machines running on Windows Server "8" Beta and want to move to the Windows Server 2012 Release Candidate—what do I need to do?
8. I notice Windows Server 2012 virtual machines have a Smart Paging File Location—what is the Smart Paging File?
9. I have Windows Server "8" Beta volumes dedepulicated. Can I just install the Release Candidate and still access my data?
10. Can I copy my customized Windows 8 and Windows Server 2012 Server Manager configuration to other users and computers?

Windows Server 2012 Articles

- New Ways to Enable High Availability for File Shares
- Microsoft Releases Windows Server 2012 to Manufacturing
- Top 10 Windows Server 2012 Storage Enhancements
- Is Microsoft Trying to Kill Windows Server?
- Getting Around in Windows Server 2012, Part 1
- Shared-Nothing VM Live Migration with Windows Server 2012 Hyper-V
- Windows Server 2012 Simplifies Active Directory Upgrades and Deployments
- Windows Server 2012 Storage Spaces
- Video: Windows Server 2012 Storage Spaces Demo
- How Windows Server 2012 Improves Active Directory Disaster Recovery
- Introducing a Simpler Windows Server
- Windows Server 2012 Will Have Feature Parity Across All Editions
- Windows Server 2012 Is Good News for IT
- Top 10 New Features in Windows Server 2012
- Understanding Windows Server 2012 Hyper-V Networking Changes
- Windows Server 2012 Active Directory Moves Forward
- Microsoft's Jeffrey Snover Discusses Windows Server 2012
- Windows Server 2012 Beta Introduces ReFS: Resilient File System
- Exploring Windows Server 2012: Dynamic Access Control
- What's New in Windows Server 2012 Active Directory
- Server Manager in Microsoft Windows Server 2012
- Windows Server 2012: A Leap Ahead

www.windowsitpro.com/windows-server-2012

Welcome to Windows 8

The new client OS offers the best of both worlds

Paul Thurrott

is senior technical analyst for *Windows IT Pro*. He writes the SuperSite for Windows, a weekly editorial for Windows IT Pro UPDATE, and a daily Windows news and information newsletter called WinInfo Daily UPDATE.

Email

Website

I'll just come right out and say it. Windows 8 is Apple's fault. We can tie the creation of Microsoft's unique, hybrid platform to Apple's decision a decade ago to branch out beyond its PC products to find a market—any market—in which the company could be more successful. Apple first moved into music, of course, which seemed like a big deal at the time. But the firm's subsequent evolution, which included forays into e-commerce, digital media ecosystems, and devices such as the iPod, iPhone, and then iPad, was a much, much bigger deal.

Today, Apple's PC business—the Mac—is successful, yes, but still an also-ran in that market. The company's other efforts have eclipsed first the Mac, and then the rest of the technology world. Apple today isn't just the biggest technology company; it's one of the biggest publically traded companies anywhere. Apple, not Microsoft, is writing the future of computing, thanks to the staggering success of the iPhone and iPad product lines. This, folks, is what's called a crisis.

What *Not* to Do

Author Michael Crichton noted more than 40 years ago that a crisis is "a situation in which a previously tolerable set of circumstances is

suddenly, by the addition of another factor, rendered wholly intolerable." From Microsoft's perspective, the almost casual way in which the company dominated the PC industry from the early 1990s onward, creating a business that was (for a time) the largest and most profitable on earth, was a tolerable set of circumstances. Microsoft was, and still is (through sheer inertia), a money-making machine. But another factor has been introduced. In this case, it wasn't Apple per se: Remember, Mac computers never seriously threatened Microsoft. No, it was the rise of simpler and more mobile computing devices, products such as the iPod, iPhone, and iPad as well as the "me-too" products that sprang up in their wake.

For Microsoft, this condition is indeed "wholly intolerable." What's amazing is that Microsoft has reacted to it so quickly. The intolerable situation—the rise of simple, mobile computing devices—is still unfolding. And Microsoft's core business of selling software that runs (and runs on) traditional PCs is still chugging along at a fairly acceptable rate. Sure, the growth is small. But for a mature market, PCs are still big business, with roughly 375 million units sold each year.

Microsoft was, and still is, a money-making machine.

There are different ways in which one can react to a crisis. When Windows Vista arrived in 2006, it was a ramshackle mess, the result of Microsoft uncharacteristically overestimating what the company could deliver and then starting over from scratch late in the game. The result was a bizarre collection of vestigial half-features from the Longhorn project and a handful of new technologies, many of which were immediately abandoned.

Microsoft should have reacted to this disaster by acting quickly, fixing the problems, and aggressively fending off repeated attacks—by Apple, in particular, which sensed the problem immediately and escalated its "I'm a Mac, I'm a PC" ads to poke incessant fun at Vista's problems. Instead, the company reacted like a hedgehog under attack. First, it remained still and hoped the problem would go away. Then it belatedly tried to protect itself with minor PR victories (e.g., the Mohave project, the "I'm a PC" campaign) that virtually no one noticed.

Windows 8 is something completely new and different.

With Vista, the crisis was real and direct, an in-your-face problem that Microsoft simply didn't respond to properly because it had grown big, complacent, and slow. Microsoft couldn't react to that crisis because it had never experienced one before. The company's previous defense—just being Microsoft, the dominant PC firm—suddenly failed it, for the first time.

Looking to today's evolution toward simple mobile computing devices, the crisis is quite different. Microsoft could easily coast for years and do pretty well, continuing to dominate the ever less relevant PC market with its hundreds of millions of units per year. But the market for smartphones, tablets, and related devices is already bigger than that for PCs. And as people turn away from PCs and toward these devices, that market is going to continue getting much bigger each year.

A Paradigm Shift

Microsoft, amazingly, is confronting this issue head-on. And the company is doing so while its best-ever-selling version of Windows, Windows 7, continues to rack up license sales of more than 20 million units per month, a steady clip that has gone essentially unchanged for three years straight. No one would look at Windows 7 and declare it to be anything other than vastly superior to its loathed predecessor, Vista.

But rather than slowly evolve Windows into something different, or develop a new mobile platform side-by-side with Windows, Microsoft has instead taken a dramatic step in releasing Windows 8. This new platform isn't the next version of Windows 7, despite Microsoft's efforts to market it as such. No, Windows 8 is something completely new and different.

Windows 8 is no less than a major new mobile platform that accomplishes two things. First, it provides the software giant with a platform that's vastly superior, out of the gate, to the two platforms that currently dominate this market: Apple iOS (running on the iPad) and Google Android OS. Second, it brings with it the previous Windows desktop platform and (for the most part) all the compatibility that

platform provides: desktop applications, utilities, hardware drivers, and so on.

Windows 8 also brings with it all the problems of the Windows desktop (or what we previously thought of simply as Windows). The complexity. The insecurity. The unreliability. The legacy deadwood—software that's still stuck in there because Microsoft has always cared more about backward compatibility than anything else. (No customer left behind!)

But this is the genius of Windows 8, really. Because there's a second version of Windows 8, Windows RT (formerly called Windows on ARM), that doesn't include any of the issues associated with legacy software. You can't install third-party desktop software on Windows RT because this platform runs on ARM rather than on the x86 or x64 underpinnings that we've used since the original IBM PC in 1981. This restriction is bad in some ways—your copy of Adobe Photoshop is never going to work on Windows RT, sorry—but good in many others. Those viruses, blue screens, and other issues are going to be non-existent—or nearly so—in Windows RT.

The new OS we should be talking about here is Windows RT, not Windows 8. Although Microsoft positions Windows RT as simply the ARM-based variant of Windows 8, the situation is in fact reversed: Windows RT is Microsoft's new mobile platform. And Windows 8 is the PC-based variant of *that* system, providing all the new stuff from RT along with backward compatibility so that the existing customer base can make the transition more easily. Put another way, Windows RT is a fresh start. Windows 8 simply bridges the old and the new.

And make no mistake, this transition is happening. If Microsoft is successful with this plan, we'll leave behind the traditional PC in the years ahead. At the very least, the Intels and AMDs of the world will evolve their own hardware platforms to be more like ARM, and Microsoft will start chopping legacy deadwood off Windows 8 and its successors. The world we're heading toward belongs to Windows RT.

Back to the Future

The thing is, we've already done this. Back in the early 1990s, just as Windows took off in the market, the software giant started a skunkworks project called NT, using disgruntled former Digital Equipment engineers and their anything-but-UNIX philosophy to create the next major OS. It took a while, but the Microsoft customer base transitioned from what we used to think of as Windows to NT; by the time Windows XP shipped in 2001, NT *was* Windows.

If Microsoft is successful in the transition from *today's* Windows to Windows RT, it will achieve the same result. We'll continue to use this thing that we call Windows. But that system, underneath, will be new, designed from scratch, and it will carry with it just enough backward compatibility to make the change easy for users—just like NT did.

Old-timers will recall that the thought of typical consumers running NT back in 1993 to 1995 or so was ludicrous. NT had heady hardware requirements and precious little compatibility with existing software and hardware. But that changed over the years, and through subsequent NT-based releases—Windows NT 4.0, Windows 2000, and Windows XP—NT went from burden to benefit. So it will be with Windows RT, although I don't think it will take as long, or as many interim versions.

These comparisons are never exact, but I'd say that Windows RT is most like NT 4.0, in that it looks and works a lot like the current mainstream Windows version and is largely compatible with current software applications and hardware. (Remember that Windows RT and Windows 8 can run the same Windows 8 apps, previously known as Metro-style apps.) So Microsoft has conceptually skipped the corresponding NT 3.1, 3.5, and 3.51 stages with this first release of Windows RT. I bet the company can get to a Windows XP–comparable release with its next version.

Speculation aside, Windows 8 represents a transition: a bridge between what was and what will be, and a way for current PC users to become accustomed to and proficient in what Microsoft calls a "touch first" user experience. The underlying platform will grow and evolve, of course, and I suspect many of the real complaints that

people have about Windows 8—and yes, there are a ton of them—will be addressed in future updates that will likely occur well before any Windows 9 release. (My sources tell me that Windows 8 won't sit still for three years, and that Microsoft is planning for yearly updates to ensure that this platform matures quickly.)

Windows 8 is the start of a revolution.

On the hardware front, Windows 8 is like previous versions of Windows in many ways. That is, yes, you can install and run Windows 8 on your existing PCs and it will work well—a lot better than the clueless tech pundits are now claiming. (In fact, looking at just the desktop, Windows 8 is an even bigger improvement over Windows 7 than that OS was over Windows Vista.) But you'll get the best results with a new PC, one that includes a touch screen or perhaps a hybrid design in which a laptop-type PC can be transformed into a tablet (or vice versa). Windows 8, like Windows RT, comes alive on these devices.

And that, really, is the point. As the world transitions to simpler, more mobile devices, Windows 8 and (to a greater extent) Windows RT give Microsoft an instant solution that in many ways is superior to what's offered by its rivals. The fact that both offer some degree of compatibility and familiarity with the Windows desktop is a bonus. You'll be able to buy iPad-class devices that transform into real PCs and can run real Photoshop, not the sad version that iPad users put up with. When you consider the amount of time, money, and effort that iPad users expend trying to make their expensive toys act more like PCs, you realize that Microsoft's strategy makes sense. It's a winner.

Change Happens

Windows 8 is the start of a revolution. It's exciting and forward leaning. Yes, it's different, but get over it: We made the transition from keyboard and command line to mouse and GUI. We can make this transition, too. In fact, rather than dread it, we should be embracing it wholeheartedly. With Windows 8—and Windows RT—Microsoft is giving us the best of both worlds. ■

InstantDoc ID 144141

Microsoft Windows 8 Arrives

The new client OS represents a radical departure from previous Windows versions

Windows 8, Microsoft's latest client OS, features a new UI designed to be tablet touch-friendly, and is available to customers via software upgrades or with new PC purchases on October 26, 2012. Windows 8 represents a radical departure from previous Windows versions and is arguably the most dramatic upgrade Microsoft has yet developed.

The system is essentially a brand-new mobile platform that has been melded onto the traditional Windows desktop, giving users what Microsoft calls a "no compromises" experience that blends the best of mobile with the best of Windows. *Windows IT Pro* brings you ongoing coverage of Windows 8, with in-depth treatment of significant features, breaking news, and analysis. Visit our Windows 8 page for the latest news and technical features. ■

InstantDoc ID 144099

Windows 8 In-Depth

- Windows 8 Upgrade Offer for PC Buyers Goes Live
- Start: The Windows 8 Era Begins
- Enterprises: Now's the Time to Get Your Windows 8 On!
- Installing Windows 8 Enterprise Edition Product Key
- Will IT Departments Rush to (or Away from) Windows 8?
- Q: Is there a version of the Microsoft Assessment and Planning Toolkit that works with Windows Server 2012 and Windows 8?
- Q: Why, when I enable .NET Framework 3.5 on Windows 8 and Windows Server 2012, does it connect to the Internet and pull down files?
- Q: Can client Hyper-V in Windows 8 run virtual machines that are stored on an SMB 3.0 file share?
- Windows 8's "Killer Feature" for Microsoft Certified Trainers
- Q: I disabled hibernation on my Windows 8 installation—so why does startup seem to take longer?

Windows 8 Features

- Windows 8 Feature Focus: Start Screen
- Windows 8 Feature Focus: Multi-Monitor
- Windows 8 Feature Focus: Tiles
- Windows 8 Feature Focus: Contracts
- Windows 8 Feature Focus: Lock Screen
- Windows 8 Feature Focus: Charms
- Windows 8 Feature Focus: Snap
- Windows 8 Feature Focus: Switcher
- Windows 8 Feature Focus: Back Tip
- Windows 8 Feature Focus: Start Tip

Windows 8 Tips

- Windows 8 Tip: Overcoming Library Limitations
- Windows 8 Tip: New Mice and Keyboards
- Windows 8 Tip: Protect Portable Storage with BitLocker To Go
- Windows 8 Tip: Customize the Start Screen
- Windows 8 Tip: Master Keyboard Shortcuts
- Windows 8 Tip: Manage Notifications
- Windows 8 Tip: Integrated Facebook and Twitter
- Windows 8 Tip: Use the Web-Based Installer
- Windows 8 Tip: Enable File History
- Windows 8 Tip: Upgrade from a Previous Windows Version
- Windows 8 Tip: Disable the Lock Screen
- Windows 8 Tip: Virtualize with Hyper-V

www.windowsitpro.com/windows-8

Enabling List Object Mode in a Forest

For secure delegation, use List Object mode to hide data in Active Directory

Guido Grillenmeier

is a chief engineer within the Enterprise Services Group at HP. He is a Microsoft Directory Services MVP, a Microsoft Certified Architect, and the coauthor of *Microsoft Windows Security Fundamentals* (Digital Press).

Email

You can make data in Active Directory (AD) visible only to those who need to see it. Hiding data allows delegated administration of users, groups, or computers to any security principal, so that many daily operational tasks don't need to be performed by domain administrators. Hiding data in AD by using normal AD permissions is one option, as I described earlier in this article series. (See the Learning Path for a list of the previous articles in the series.) Another option, and the one I'll examine in this article, is to enable List Object mode (sometimes referred to as List Mode) in the AD forest. (Later in the series, I'll tell you about a third option: adjusting the default security descriptor of AD objects.)

List Object Mode

As I mentioned in my previous articles, Authenticated Users are granted the Read and List Object permissions on any newly created organizational units (OUs). In its default configuration, AD doesn't enforce the List Object permission, and the AD security editor doesn't display the permission. However, after an enterprise administrator enables List Object mode (which can be enabled only for the entire forest), the List Object permission is enforced. I'll cover how to enable List Object mode later in this article, but first let's concentrate on how this mode works.

It's crucial to understand the difference between the List Contents and the List Object permissions and how they work together. The concept of List Object mode is quite simple. When this mode is disabled (which

it is by default), AD doesn't evaluate the permissions of any objects underneath any container object (e.g., an OU) that a user queries.

To view the contents of an OU, the user needs to be granted the List Contents permission (which is a subset of the Read permission) on the OU. If the List Contents permission isn't granted (e.g., because the Read permission is removed), then no child objects are returned to the user. If the List Contents permission is granted, then AD returns all child objects of the OU to the user, regardless of whether the user has the Read permission on, or is denied access to, the child object. However, a GUI such as the Microsoft Management Console (MMC) Active Directory Users and Computers snap-in can't correctly display the object type unless the user has Read access on a child object. Instead, the type is displayed as Unknown, as Figure 1 shows.

When List Object mode is enabled, AD evaluates the permissions of each object before returning the list of objects to a user. Administrators can remove or deny the List Contents permission on a parent container, to hinder the return of all child objects in the respective container. But AD still processes the permissions on those child objects to determine whether the user has been granted the List Object permission on any child object. If so, AD adds the object to the result set; if not, the object is omitted.

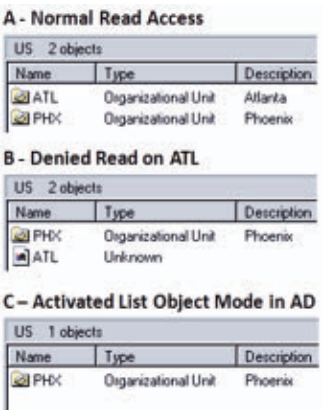


Figure 1
Displaying Objects in List Object Mode

The three example situations in Figure 1 show the difference between using List Object mode and using normal permissions to hide objects in AD:

- Situation A (Normal Read Access)
  - o List Object mode in AD is turned off.
  - o The user is granted the List Contents permission on the US parent OU, via the normal Read permission that's granted to Authenticated Users.

  - The user also has the Read permission on child objects (i.e., the ATL and PHX OUs).
  - The result is that two objects are displayed in Active Directory Users and Computers. The UI can evaluate both objects, which can be displayed with the correct icon and so on.
- Situation B (Denied Read on ATL)
  - List Object mode in AD is turned off.
  - The user is granted the List Contents permission on the US parent OU, via the normal Read permission that's granted to Authenticated Users.
  - The user still has Read permission on the PHX child object, but Read access to the ATL child object is removed for Authenticated Users.
  - The result is that two objects are displayed in Active Directory Users and Computers, but the UI can correctly evaluate and display only the PHX child object; ATL is displayed as an unknown object, although the user knows that the object exists.
- Situation C (Activated List Object Mode in AD)
  - List Object mode in AD is turned on.
  - The List Contents permission on the US parent OU is removed for the user, by removing the permission for Authenticated Users.
  - The user has the default Read and List Object permissions on the PHX child object. The user still has the default Read permission on the ATL child object, but the List Object permission is removed.
  - The result is that only one object—the one to which the user has the List Object permission—is displayed in Active Directory Users and Computers. Because of the additional Read permission on other attributes, the UI correctly evaluates and displays the object. The ATL child object is no longer displayed, and the user doesn't know about its existence in AD.

The List Object permission is a useful tool when users aren't supposed to see certain objects in AD. The permission is typically used on OUs, to fully remove an OU's visibility for all users (with the exception of the administrator who is managing the OU). The List Object permission is mostly helpful in outsourcing environments, in which the outsourcer hosts a directory for multiple companies and the users or OU admins of each company shouldn't see the OU for the other companies.

Within an organization, the List Object permission is often used to hide security-sensitive objects, such as admin accounts, from unauthorized users. Doing so limits the potential for Denial of Service (DoS) attacks against these accounts.

As previously mentioned, the List Object permission isn't active or visible in AD's security editor until List Object mode is enabled in the forest. When this feature is enabled, a new permission appears in the AD security editor, as Figure 2 shows.

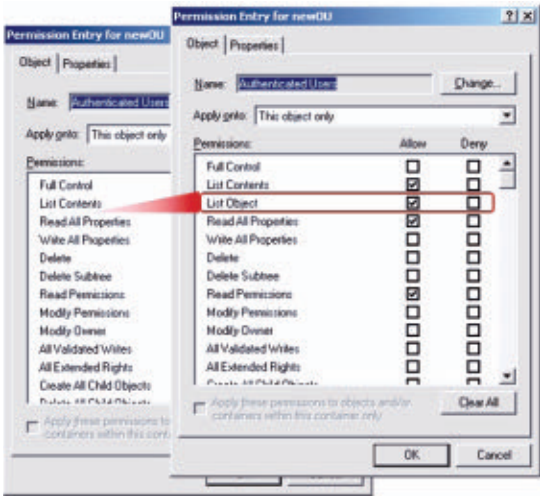


Figure 2
Active Directory Security Editor, Before and After Enabling List Object Mode in Active Directory

Enabling List Object Mode

To enable AD's List Object mode, you must edit a property of the Directory Services object in the AD configuration container, which requires Enterprise Admin privileges. This change is automatically replicated to all other domain controllers (DCs) in the forest. You can't activate List Object mode on a per-domain basis.

List Object mode is activated by setting the third character (byte) of the DSHeuristics property (Unicode string syntax) on the Directory Service object to 1. If the DSHeuristics property hasn't been set with other

values, set it to 001. If the first two characters, or bytes, are already set to a non-zero value, leave them as they are. The Directory Services object is in the AD container cn = Directory Service,cn = Windows NT, cn = Services,cn = Configuration,dc = ForestRootDomain.

Other DSHeuristics settings on the Directory Service object are used to control name resolution during AD searches, for example. When enabled, the List Object permission must be administered in conjunction with the List Contents permission. Table 1 summarizes the rules for using List Object mode with the List Contents permission.

The goal of the next permission example is to use the List Contents and List Object permissions appropriately to set up OU permissions for a company that runs an outsourcing business for multiple customers (see Figure 3). In this context, it's very important that only authorized users (i.e., members of the UserAdmins_CompanyX groups) can view their respective OU (i.e., CompanyA, CompanyB, or CompanyC), including the content under the UserAccounts parent OU. Setting up this scenario involves the following steps:

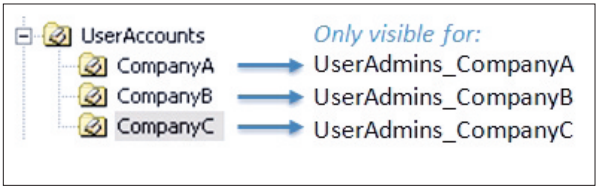


Figure 3
Setting OU Permissions for Multiple Customers

1. Remove the default List Contents permission for Authenticated Users from the UserAccounts OU. Doing so triggers the evaluation of child object permissions. (For information about how to perform this step, see the previous article in this series, "Hiding Active Directory Objects and Attributes.")
2. Remove the default List Object permission for Authenticated Users from all company OUs, to hide the visibility of the company OUs. In addition, remove the List Contents permission from the OU, to hide the objects within the OU. (As a result, these objects won't be returned during a subtree search.)
3. Grant the List Object and List Contents permissions for each UserAdmins group on the respective company OU.

Table 1: Rules for Using List Object and List Contents Permissions

Granted Permissions On...		Result
OU	Child Objects	
List Contents and List Object	N/A	The List Object permission on the OU makes the OU visible. Because List Contents is also granted on the OU, this permission takes precedence over any missing List Object permissions for child objects, and AD automatically lists all objects in the container.
		A delegated administrator can browse to the OU and to all child objects by using Active Directory Users and Computers.
		An LDAP query for all objects returns the OU and all child objects.
List Object (List Contents not granted or denied)	List Object	The List Object permission on the OU makes the OU visible. If the List Contents permission isn't granted or is denied and the List Object permission is granted on the container object (e.g., an OU), then AD evaluates the List Object permission for the child objects and lists only those on which the List Object (or Read) permission has been granted.
		A delegated administrator can browse to the OU and selected child objects by using Active Directory Users and Computers.
		An LDAP query for all objects returns the OU and only those child objects on which List Object permission has been granted.
List Contents (List Object not granted or denied)	N/A	The OU isn't visible. Because the List Contents permission is granted on the OU, this permission takes precedence over any missing List Object permissions for child objects, and AD automatically lists all objects in the container.
		A delegated administrator can't browse to the OU or child objects by using Active Directory Users and Computers.
		An LDAP query for all objects doesn't return the OU object but does return all the OU's child objects.
Neither List Contents nor List Object	N/A	The OU isn't visible. Because neither the List Contents nor List Object permission is granted to the container object (e.g., an OU), AD doesn't evaluate any permission on the child objects.
		A delegated administrator can't browse to the OU or child objects by using Active Directory Users and Computers.
		An LDAP query for all objects doesn't return the OU or any of its child objects.

DSACLS Example

Although the List Contents and List Object permissions can be set from the AD security editor, it's much easier to use the Dsacls command-line tool to set the permissions for multiple OUs. To do so in this example scenario, enter the following command, which first removes all permissions for Authenticated Users and then grants the required Read permissions on the OU without the List Contents permission:

```
set DN="OU=UserAccounts,DC=root,DC=net"&& set SP=
  "Authenticated Users"&& DSACLS %DN% /R %SP%&&
  DSACLS %DN% /G %SP%:RCRPLO
```

The goal of Step 2 is to remove the default List Object and List Contents permissions for Authenticated Users from all company OUs. As when using Dsacls to remove the List Contents permission only, this step involves first removing all permissions for Authenticated Users and then resetting the permissions that you want to keep (in this case, Read and Read All Properties). For a single OU in our example scenario, use this command:

```
set DN="OU=CompanyA,OU=UserAccounts,DC=root,
  DC=net"&& set SP="Authenticated Users"&&
  DSACLS %DN% /R %SP%&& DSACLS %DN% /G %SP%:RCRP
```

For multiple OUs, creating a list of distinguished names (DNs) and saving them to a file is easier. You can do so by using Dsquery:

```
DSQUERY ou <StartNode> -scope onelevel > queryresult.txt
```

In our example scenario, the command would look like this:

```
DSQUERY ou "OU=UserAccounts,DC=root,DC=net" -scope onelevel >
  queryresult.txt
```

After verifying the validity of your query results, you can perform a FOR loop to execute the previous Dsacls command against all objects in the file:

```
for /f "delims=" %I in (queryresult.txt) do set SP=
  "Authenticated Users"&& DSACLS "%~I" /R %SP%&&
  DSACLS "%~I" /G %SP%:RCRP
```

Note that to use the For command in a batch program, you would specify %%I instead of %I.

In Step 3, the actual permission to view the correct OU and its contents must be granted to the respective UserAdmins group for each company, by granting the List Object permission to the correct group:

```
DSACLS <DN of object> /G <security principal>:LOLC
```

In the example scenario, the command would look like this:

```
DSACLS "OU=CompanyA,OU=UserAccounts,DC=root,DC=net" /G
  "UserAdmins-CompanyA":LOLC
```

Note that setting the List Contents permission next to the List Object permission for this OU ensures that all objects in the OU are returned for the authorized users. If the goal is to further distinguish which objects within the OU should be returned during a query, then the List Contents permission should not be set. In this case, the List Object permission would be required on each child object to list the object.

Using a For loop, you can also automate the previous step by using

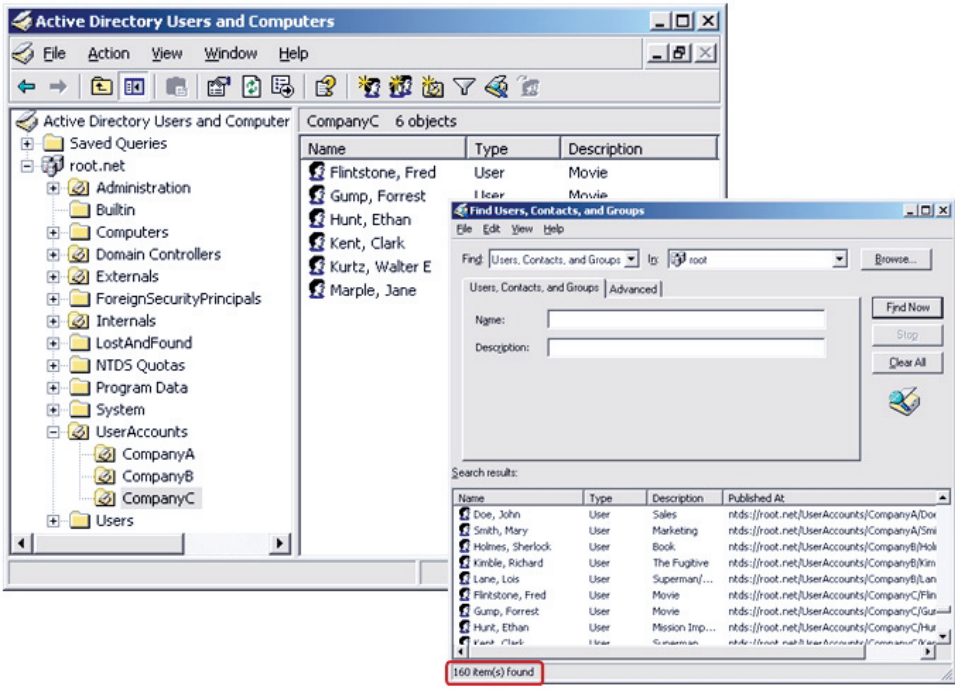
```
for /f "delims=" %I in (companylist.txt) do DSACLS "OU=%~I,OU=
  UserAccounts,DC=root,DC=net" /G "UserAdmins_%~I":LOLC
```

where companylist.txt contains a flat list of company names.

The result of the previous permission example is effectively to hide all user accounts of any hosted company in AD from unauthorized users. Members of the respective UserAdmins_CompanyX group can now view only the accounts from their company. The permissions for a company's UserAdmins group can be further extended to allow appropriate delegated admin functions (e.g., password resets).

To effectively hide all other objects in the AD domain—such as the Builtin, Computers, System, and Users containers, or any other container object—from users other than Domain Admins, remove the List Contents permission for Authenticated Users from the domain object itself (e.g., root.net). Then, remove the List Object permission for Authenticated Users for any container that should be hidden. Domain Admins (as well as Enterprise Admins) will still have full access to all objects through their respective groups' other inherited or explicit permissions on the OUs. Figure 4 and Figure 5 show the results.

Figure 4
Viewing Hidden OUs as Domain Admin



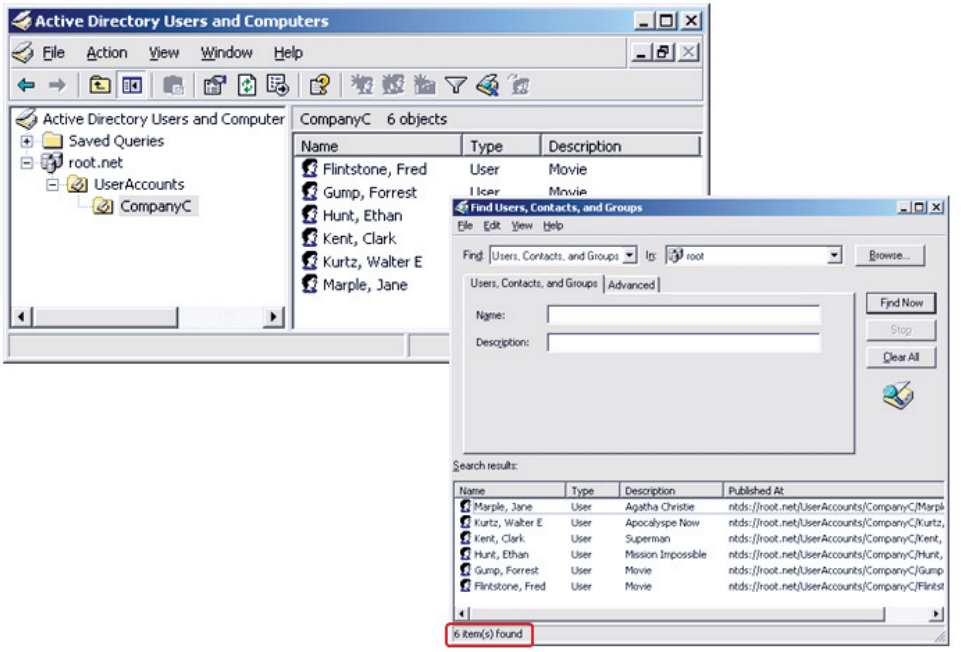


Figure 5
Viewing Hidden OUs as UserAdmin of CompanyC

Changing the visibility of objects in AD in this way can also affect other applications that leverage AD. These applications might rely on permissions that are granted to Authenticated Users. In other words: Testing is required to evaluate the effect of hiding OUs in an AD domain.

In a hosted Exchange Server environment, this approach works well because the Exchange servers are granted their own special rights on objects. Nevertheless, further adjustments are required to appropriately display address lists to users. You can typically disable the Global Address List (GAL) and create company-specific address lists instead, using an LDAP filter that points to the company OU only.

List Object mode in AD, which has been available since Windows 2000, can be compared with the Access-Based Enumeration (ABE) file-system feature that was introduced in Windows Server 2003 Service Pack 1 (SP1). By default, the normal NTFS file-system permissions on folders allow a user who has Read or List permissions on the folder to see all files and subfolders, regardless of whether the

"Hiding Data in Active Directory"
"Hiding Active Directory Objects and Attributes"

user has permissions to open the files to read them. When ABE is activated on a share, the file server evaluates the user's permissions for every file or subfolder, before returning the list of objects to the user. There's no dedicated List Object permission for files and folders in NTFS, so a user requires at least Read permission to view a file or folder in an ABE-enabled share.

In any case, these are the most important things to remember when working with the List Object mode in AD:

- List Object mode can be enabled only for an entire AD forest; you can't enable this mode per domain.
- To leverage the List Object permission on child objects, you should remove the List Contents permission for Authenticated Users from the respective parent container. If a user is granted the List Contents permission on a container object, then the objects therein are visible regardless of the underlying List Object permissions of the child objects.
- Enabling List Object mode doesn't add any features to hide attributes in AD. The mode's sole purpose is to allow the setting of more granular permissions for listing objects within container objects so that only authorized users can view them.

Understand the Tasks

If you've read all the articles in this series, then you know that hiding data in AD can be a daunting task. Understanding the default permissions that are applied to objects in AD is crucial for any permission change, especially before tackling the use of List Object mode.

The last basic type of permission configuration option to be aware of is the default security descriptor of objects in AD, which I'll discuss in the next article in this series. I'll then finish off with a few advanced topics on handling built-in property sets and on handling AD attribute permissions with the confidentiality bit and with the filtered attribute set (FAS). ■

InstantDoc ID 143899

Deconstructing the Hybrid Configuration Wizard in Exchange Server 2010 SP2

Peek under the hood for a better understanding of your hybrid environment

Jorge R. Diaz

is a cloud solutions architect at Planet Technologies, focusing on Office 365 for state and local government and higher education institutions. He's also a technical editor for Microsoft Press books on Office 365.

Email

Twitter

LinkedIn

Website

Blog

For those of us working in the cloud, the most exciting feature of Microsoft Exchange Server 2010 Service Pack 2 (SP2) is the Hybrid Configuration Wizard (HCW). Prior to SP2, the process for configuring the necessary connections to enable interoperability between an on-premises Exchange environment and Microsoft Office 365 was daunting. Even with the Exchange Server Deployment Assistant (aka ExDeploy), you needed 65 pages of detailed instructions and guidance that included somewhere in the neighborhood of 60 steps (depending on your configuration) to complete an on-premises infrastructure for a successful hybrid deployment—or just to make on-premises servers communicate properly with Exchange Online.

Enter Exchange 2010 SP2, which includes the masterfully designed HCW. The HCW simplifies the configuration process to fewer than 10 clicks of a mouse. (The exact number of steps varies depending on whether you plan to use centralized or direct mail flow, whether you'll use full hybrid mode or online archiving, and the amount of free/busy sharing.) Many were ecstatic when Microsoft released the wizard, and we anxiously installed it on our systems. To date, the wizard has come through on its promise to simplify and automate hybrid deployments, with little input required from the systems administrator.

Although I applaud Microsoft's accomplishment, I worry about future administrators who will never have the chance to trudge

How will administrators know how to troubleshoot problems if they don't understand the multitude of configuration changes that the hybrid wizard is executing?

through a manual hybrid deployment. For administrators who haven't lived in a pre-SP2 world, the complexities of what the wizard does in the background will be lost. Ultimately, problems could result for organizations if something within the Exchange federation or organization relationship (e.g., free/busy lookups, centralized mail flow) breaks. How will administrators know how to troubleshoot problems if they don't understand the multitude of configuration changes that the hybrid wizard is executing while they happily click Next?

In this article, I'll explain what's under the hood of the HCW as well as which changes are made (from an architectural standpoint) to simplify the deployment scenario and increase the success rate of hybrid deployments. (This article assumes that you've previously deployed Active Directory Federation Services—ADFS—and the Microsoft Directory Synchronization Tool but doesn't go into detail about those configurations, which are beyond the scope of the article.) I'll also provide some guidance for administrators to overcome problems that they might encounter during the process. Let's dive in!

Some Background on the Architectural Changes

The first thing to look at is the use of DNS namespaces for mail routing and federated delegation. Prior to SP2, Microsoft required that to facilitate the relationship between your on-premises and Office 365 environments, you had to implement two additional namespaces:

- exchangedelegation.domain.com
- service.domain.com

The exchangedelegation namespace was used to create an Exchange federation between the on-premises Exchange environment and Office 365. The term *federation* is widely used and can often confuse administrators. In this context, we're talking about Exchange federation, which is used to help Exchange and Office 365 share information. This type of federation uses the Microsoft Federation Gateway and federation trusts to share information, such as calendar free/busy data and MailTips.

The service namespace was used as a secondary accepted domain, to route mail from the on-premises environment to Office 365.

A common question that Exchange administrators asked when this solution first came out was simply, Why are two additional namespaces required when Office 365 uses a domain.onmicrosoft.com namespace for each tenant domain? There really was no good answer. Microsoft developed this method, which seemed to work but proved to be inefficient and fragile in production. Microsoft addressed the issue in SP2 by no longer requiring these namespaces. Instead, SP2 uses the onmicrosoft.com namespace, which Office 365 assigns and manages, for mail routing. In addition, Exchange federation is now established at the root domain.com. You can forget about both of the aforementioned namespaces. Although this domain consolidation isn't exactly part of the HCW, it's worth noting before you launch the wizard.

Now that we've covered the DNS improvements, let's explore the HCW itself, examining each step.

Launching the Wizard

Before running the HCW, you must add the Office 365 tenant to the on-premises Exchange Management Console (EMC). HCW executes several Windows PowerShell cmdlets and requires an established remote PowerShell session, which EMC generates when you add your cloud tenant. After doing that, you can find the wizard under Organization Configuration in the On-Premises section of the EMC.

The next step is to create an HCW object by clicking New Hybrid Configuration in the Actions pane, as Figure 1 shows. This first step might appear to simply create an unconfigured object, but it actually executes several PowerShell commands that generate a new self-signed certificate and a new federated trust between the on-premises Exchange environment and the Microsoft Federation Gateway. The final step in creating the new HCW object creates the environment to allow the full HCW to run later. From a PowerShell perspective, the following commands are executed during this first phase:

```
New-ExchangeCertificate -DomainName 'Federation'
  -FriendlyName 'Exchange Delegation Federation' -KeySize
  '2048' -Services 'Federation' -SubjectKeyIdentifier
  '<sample key>' -PrivateKeyExportable $true
New-FederationTrust -Name 'Microsoft Federation
  Gateway' -Thumbprint '<thumbprint>' -SuppressDnsWarning
New-HybridConfiguration
```

After these commands execute successfully, you'll see the Hybrid Configuration object in the Organizational Configuration section of the EMC.

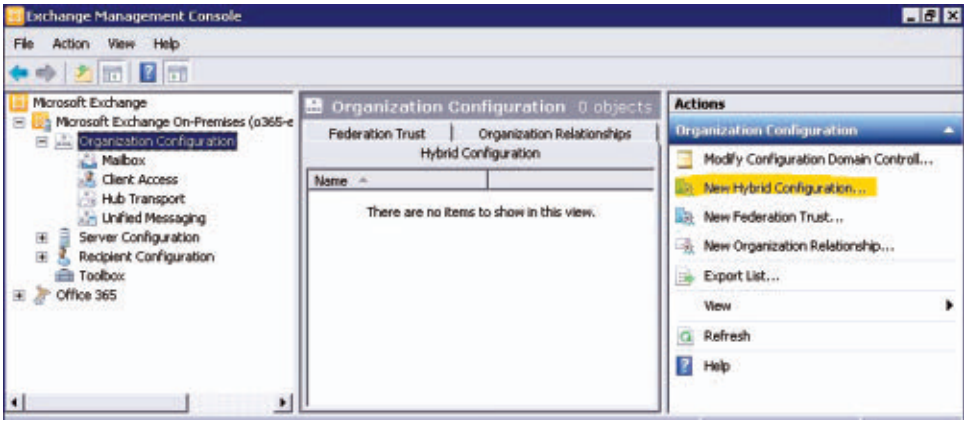


Figure 1
Adding the Hybrid Wizard Object

As you step through the wizard, several pages gather administrator input and are then used to execute the configuration commands in the background. The first page gathers on-premises and cloud credentials. These credentials must have the appropriate administrative rights on each side. The on-premises account must be a member of the Organizational Admins security group, and the Office 365 credentials must be a member of the Global Admins group within your Office 365 tenant, as Figure 2 shows.

The next page compares the list of on-premises accepted domains to the domains that are listed in the Office 365 tenant. If a domain name matches, then it can be added as the namespace that's being configured. For organizations with more than one accepted domain,

you can select all the domains you want to add that will be part of your hybrid configuration, as Figure 3 shows. Note that the domain must be validated in Office 365 before it shows up in this list.

The next page provides a text file, which you'll use to prove ownership of the domain (i.e., domain proof), as Figure 4 shows. Copy this text to the clipboard and create a DNS TXT record within your public DNS zone file. Be sure to select the box to confirm that the TXT record has been created in the public DNS. Microsoft uses this TXT record to verify that you own the public DNS namespace. Only authorized

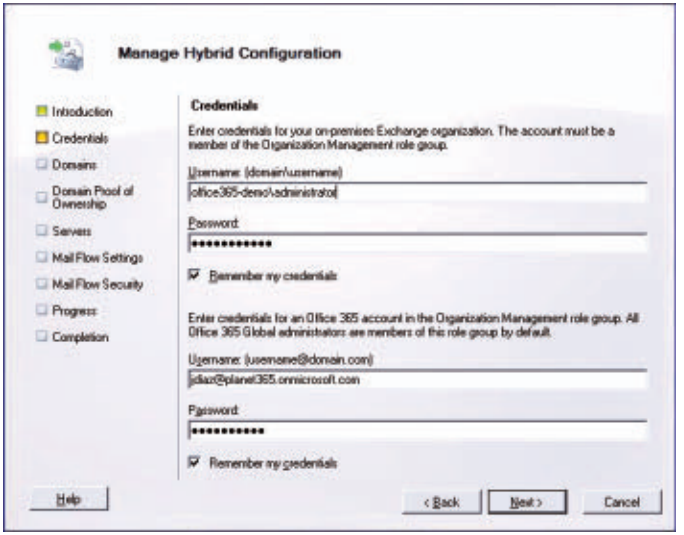


Figure 2
Providing Credentials

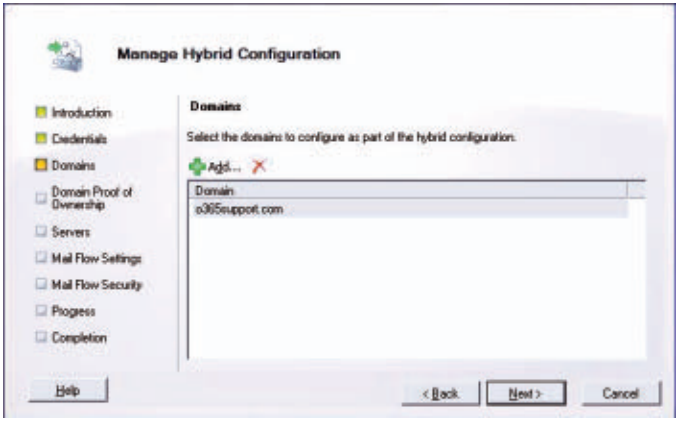
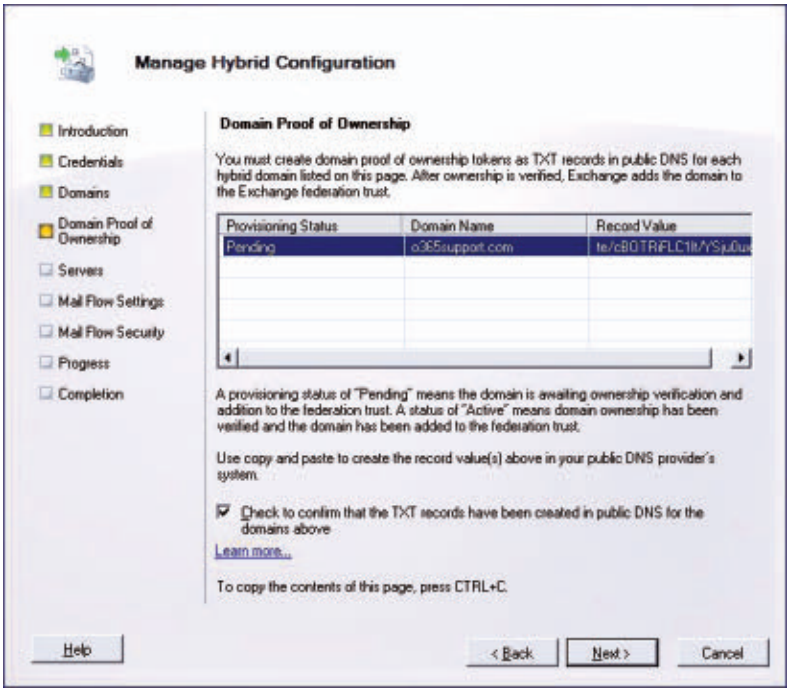


Figure 3
Selecting Domains to Add to the Configuration

Figure 4
Proving Domain Ownership



administrators have the right to change public DNS records for your zone, so adding this record proves to Microsoft that you're authoritative for your domain namespace.

On the Manage Hybrid Configuration Servers page, which Figure 5 shows, you can select the Client Access and Hub Transport servers that will be used for mailbox moves, sharing, and hybrid mail flow. Depending on the existing on-premises environment, the selection of servers might vary. If your environment already has Exchange 2010 in place, select the Client Access and Hub Transport servers that are in your primary site and have the most available resources. Your servers should have the appropriate amount of memory, CPU, and disk space. In my experience, a dual-core 3GHz processor and 8GB of RAM is generally more than enough processing power. Also, depending on the length of time you plan to be in coexistence, you might consider running multiple Client Access and Hub Transport servers in an array, for fault tolerance. Doing so will ensure business continuity if a server fails.

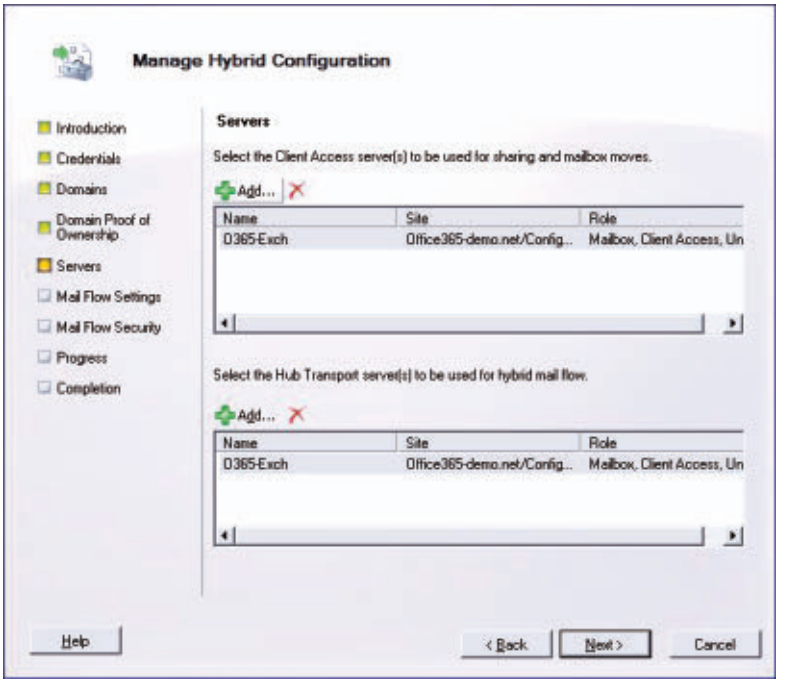
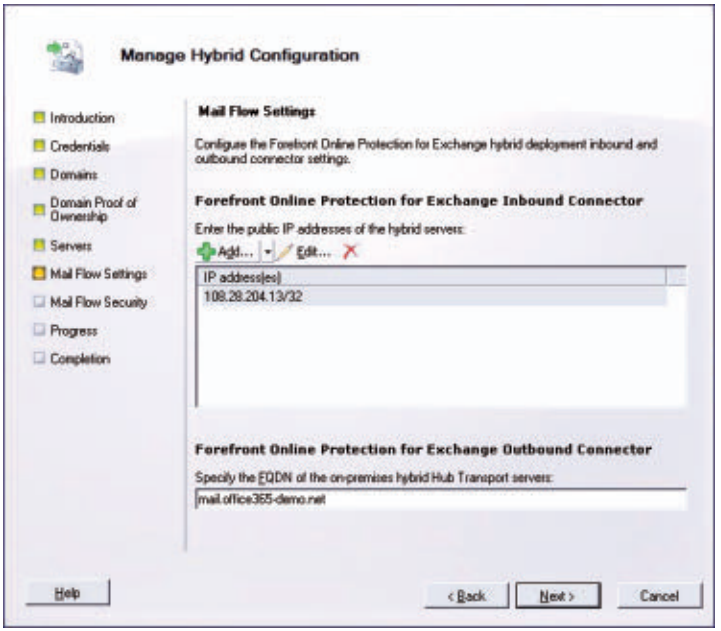


Figure 5
Servers Page

Your hybrid server(s) should be located in the same Active Directory (AD) site as your existing Exchange farm and can't reside in a demilitarized zone (DMZ). In addition, if you have Exchange Server 2003 in your environment, you'll want to add the Mailbox role to one of your hybrid servers. This server will host the free/busy replica and allow for free/busy lookups between your Exchange 2003 users and Office 365 users. Exchange 2003 uses the legacy public folder hierarchy to provide users with free/busy lookup services. Exchange 2010 (and Exchange Server 2007) changed the way free/busy lookups are handled, introducing the Availability service, which provides a more robust method for providing these lookups. For free/busy lookups to work in a hybrid environment after the Mailbox role has been installed on the Exchange 2010 hybrid server, create a public folder database and move the free/busy calendar to the Exchange 2010 server. The hybrid server will then act as the intermediary lookup between the legacy Exchange 2003 environment and the Office 365 environment.

The Manage Hybrid Configuration Mail Flow Settings page, which Figure 6 shows, requires the public IP address and Fully Qualified Domain Name (FQDN) of the on-premises hybrid server. The assumption is that the FQDN is assigned to the IP address that's listed on this page. Later, you'll see how these settings are used to configure inbound and outbound Microsoft Forefront Online Protection for Exchange (FOPE) connectors.

Figure 6
Mail Flow Settings Page



The Manage Hybrid Configuration Mail Flow Security page, which Figure 7 shows, queries Exchange 2010 Hub Transport servers for any installed certificates and allows you to select which server you want to use for the hybrid configuration. This certificate should be a publicly signed certificate from a source such as VeriSign or GoDaddy. The certificate is used for Transport Layer Security (TLS) authentication between FOPE and the on-premises server. This is also the page on which you can set the mail flow options:

- Route all mail originating from Office 365 back through your on-premises server (centralized mail flow).
- Route all mail directly from Office 365, using DNS.

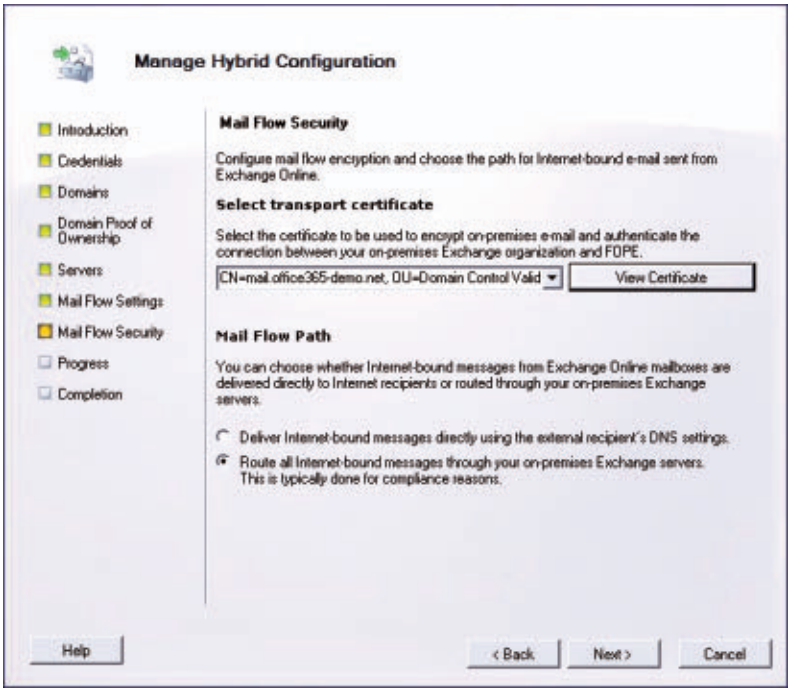


Figure 7
Mail Flow Security Page

The default selection is to use DNS rather than centralized mail flow, but be sure to update the setting according to your strategy. By centralizing mail flow, you allow administrators to track messages more easily, because all messages come through the hybrid server.

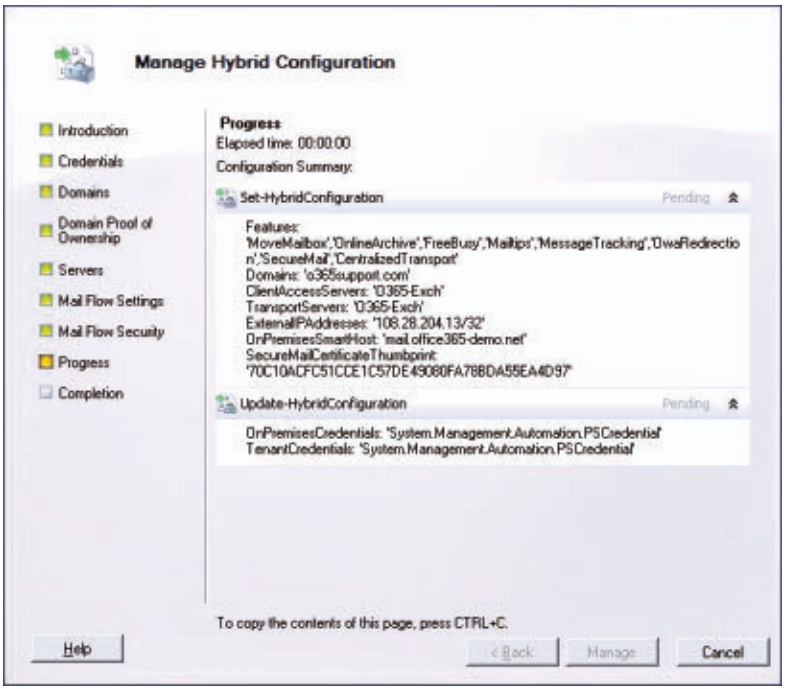
An important and often overlooked item when selecting the mail flow option is the Sender ID Framework (SPF) record. The Sender ID Framework is an authentication technology protocol that helps protect mail servers from spoofing and phishing, by verifying the domain name from the message sender. The framework validates the origin of email messages by verifying the IP address of the sender against the alleged owner of the sending domain. If your organization uses SPF records, it's important to note a few points. First, if centralized mail flow is configured, all mail appears to come from the on-premises server; no updates to SPF records need to be made. However, if you intend for your Office 365 users to send messages directly to the Internet, then you must add the Office 365 SPF values. Microsoft has

published a Sender ID Framework SPF Record wizard to help you craft your record. As an example, this is what an SPF record might look like if you choose to route mail from your on-premises environment and Office 365, assuming that your mail server's public DNS name is mail.domain.com:

```
v=spf1 a mx:mail.domain.com include:outlook.com ~all
```

The final page, which Figure 8 shows, is a summary that details the selected features, based on your input in the wizard. Click Manage to execute the wizard, and wait for the magic to happen!

Figure 8
Progress Page



Under the Hood

As you can see, the wizard makes creating a hybrid deployment very simple. It requires minimal input from the administrator and converts that input into a series of PowerShell commands that builds your configuration without further administrative input. You can imagine

how administrators might take the wizard for granted. So what really happens after you click Manage? Let's take a look. This example uses my demo tenant office365support.com. The specific values in your environment will vary, depending on your domain and DNS records. (For those of you who've deployed the wizard, you can follow the process by reviewing the log in \%ExchangeInstallPath%\Logging\Update-HybridConfiguration.)

First, the wizard establishes remote PowerShell sessions by authenticating with both the on-premises and cloud tenants. After the sessions have been established, a series of Get commands grab information from the on-premises server and Office 365. (Note that most of these commands run twice: once in the local environment and once on the Office 365 tenant.) These commands run against each of the servers that you selected in the wizard, gathering all the necessary information to begin creating the hybrid relationship.

The next set of commands attempts to configure legacy Exchange support by digging into the servers to determine where the free/busy calendar folder resides. If you look through the logs in this section, you might see an error like this one: *ERROR:System.Management.Automation.RemoteException: 'Server2' does not have the right Exchange Server version or role required to support this operation.* You don't need to worry about this error; the hybrid wizard is simply trying to determine which server is the appropriate one to host the free/busy replica.

In environments that include Exchange 2003, the wizard continues to iteratively review each server to determine whether it hosts the free/busy replica. This step is important because of the inherent difference in free/busy lookups between Exchange 2003 and Exchange 2010. The free/busy replica must reside on the Exchange 2010 server that acts as the intermediary between the legacy Exchange 2003 mailboxes and the cloud-based mailboxes. Without the free/busy public folder, users on Exchange 2003 can't see the free/busy information for cloud users, and vice versa.

After the wizard fetches the email address policy and version, it upgrades that information and adds the necessary email aliases for

mail flow—specifically, adding @domain.mail.onmicrosoft.com as an alias to all users. This step is extremely important for mail routing. During the migration process, after a user has been migrated to the cloud, @domain.mail.onmicrosoft.com is set as the routing address. From that point forward, when an attempt is made to deliver a message to the mail user on premises, Exchange uses the Route To address to forward the message to the cloud-based account by using a scoped routing connector that's created in a subsequent step.

Next, the wizard checks prerequisites within your organization and inside your Office 365 tenant, before creating organizational relationships. This step enables organization customization, which allows the wizard to build the organizational relationships. As you walk through the wizard log, you'll see multiple lines for this process. This extremely important step creates a relationship object on both sides of the federated trust, allowing these important hybrid functions:

- free/busy lookups
- MailTips
- archive access
- Outlook Web App (OWA) redirection
- delivery reports
- autodiscovery of URLs

The final phases of the process include the configuration of the Send and Receive connectors in Exchange. This phase also configures the inbound and outbound server settings within the FOPE service. Before configuring the connectors, the HCW gets the set of datacenter IP addresses that are used for the tenant and the Exchange certificate that's being used:

```
Get-HybridMailflowDatacenterIPs
Get-ExchangeCertificate -Thumbprint
  'EC0E8A739282093930AF8930E93076428CA129' -Server 'Server1'
```

The next step, which Listing 1 shows, grabs the existing connector information and creates new connectors to allow mail flow to and from Office 365. As you can see in this relatively simple example, the wizard executes 53 commands to implement the hybrid configuration that you, as an administrator, defined in less than 10 pages. Although the wizard is an amazing step forward for hybrid environments, it's inherently dangerous for inexperienced administrators who don't understand the changes being made or their purpose.

Listing 1: Creating New Connectors

```
Set-ReceiveConnector -Identity
  'Server1\Inbound from Office 365' -Name
  'Inbound from Office 365' -RequireTLS 'True'
  -PermissionGroups 'AnonymousUsers' -Fqdn
  'mail.montgomerycountymd.gov' -TLSDomainCapabilities
  'outlook.com:AcceptOorgProtocol' -Bindings
  'Microsoft.Exchange.Data.MultiValuedProperty`
  1[Microsoft.Exchange.Data.IPBinding]'
  -RemoteIPRanges 'System.Collections.Generic.List`
  1[Microsoft.Exchange.Data.IPRange]' -AuthMechanism 'Tls'

Set-HybridMailflow -SecureMailEnabled 'True'
  -CentralizedTransportEnabled 'True' -OnPremisesFQDN
  'mail.o365support.com' -CertificateSubject
  'mail.o365support.com' -InboundIPs
  'Microsoft.Exchange.Data.IPRange[]' -OutboundDomains
  'Microsoft.Exchange.Data.SmtpDomainWithSubdomains[]'
```

Common Issues and Recommendations for Getting Past Them

The HCW runs flawlessly—most of the time. However, I've encountered an issue in which the Get-FederationInformation command

times out. As a workaround, open a separate PowerShell instance and connect to your Office 365 tenant, using the same Global Admin credentials that you specified in the wizard. When the new session is established, the wizard resumes.

The problem might also be related to the Windows Communication Foundation (WCF) and Windows Workflow Foundation (WF); repairing the WCF and WF components by running the following command in the C:\Windows\Microsoft.NET\Framework\v3.0\Windows Communication Foundation directory might solve the problem:

```
ServiceModelReg.exe -r
```

Other common reasons for the HCW to fail are generally related to

- firewall restrictions
- WCF errors
- incorrect Exchange 2010 configuration:
  - o invalid Send and Receive connectors
  - o incorrect certificates
  - o missing security patches
- invalid or incorrect DNS records
- missing or incorrect permissions

Firewall restrictions are often the root cause of many mail-flow issues. As I mentioned in the beginning of the article, preplanning and testing are the keys to success. You should make a solid plan before you connect to your first server. (Speaking of plans, check out the Exchange Server Deployment Assistant. This tool helps you plan out your deployment, based on your specific environment and requirements.) A solid plan should include planning out all the IP addresses that are to be used in the hybrid deployment. After you've identified those IP addresses, you can configure the firewall to allow the appropriate traffic flow to and from those addresses. One common problem that I hear from customers and other IT professionals

is that the list of IP addresses can be difficult to find, as well as confusing. I've found the most comprehensive list of IP addresses in the Microsoft article "Office 365 URLs and IP address ranges."

DNS records are also a source of pain for many engineers trying to deploy the hybrid solution. A fellow MVP, Loryan Strant, developed an excellent Office 365 testing site to determine whether all DNS records are configured properly. Note that this site assumes that you want mail to flow from Office 365. If you use the site to test your IP addresses and want mail to flow from your on-premises mail system, you can ignore the DNS record for the cloud-based Autodiscover.

Many other common problems are related to misconfigurations within the existing Exchange environment. Several tools can help identify such issues. The Exchange Best Practices Analyzer is an excellent tool to start with. This tool reviews all your crucial components to ensure that they're configured according to best practices and provides links for items that are out of compliance.

The following resources can provide invaluable information as you plan and execute your hybrid deployment:

- Office 365 URLs and IP address ranges
- Microsoft Remote Connectivity Analyzer
- Microsoft Office 365 Deployment Guide for Enterprises
- Office 365 Community

Insight for Admins

Hopefully, this article sheds some light on how crucial it is to understand what's going on under the hood in the HCW. As I stated at the beginning of the article, I applaud Microsoft for making this process easy, but I hope that all administrators will go beyond the shiny GUI and dig deep into what happens behind the scenes. ■

InstantDoc ID 143349

OCT 29 - NOV 1 • BELLAGIO • LAS VEGAS, NV

WINCONNECTIONS
conference and expo

CLOUD CONNECTIONS · WINDOWS CONNECTIONS · Microsoft Exchange CONNECTIONS · SQL Server CONNECTIONS · SharePoint CONNECTIONS

QUESTIONS **ANSWERED** • STRATEGY **DEFINED** • RELATIONSHIPS **BUILT**

Hear what past attendees are saying about Connections...

A SAMPLING OF SPEAKERS

Make Connections the conference you bring your whole team to this year!

JIM McBEE
ITHICOS SOLUTIONS

MICHAEL OTEY
WINDOS IT PRO & SQL SERVER MAGAZINE

DON JONES
CONCENTRATED TECHNOLOGY

MARY JO FOLEY
ALL ABOUT MICROSOFT

PAUL THURROTT
WINDOWS IT PRO

KIMBERLY TRIPP
SQLSKILLS.COM

PAUL S. RANDAL
SQLSKILLS.COM

REGISTER TODAY! www.WinConnections.com • 800.438.6720 • 203.400.6121

Updating a Scheduled Task's Credentials

Use this PowerShell script to overcome Schtasks limitations

The Task Scheduler service in Windows Vista and Windows Server 2008 and later has been updated with greater functionality. However, the OSs' Schtasks tool, which ostensibly lets you manage scheduled tasks from the command line, hasn't kept up. You can no longer use the Schtasks command to update a scheduled task's stored credentials, as you could in earlier versions. This issue becomes a significant problem if the password changes for an account that's used to run numerous scheduled tasks. In this article, I'll present a Windows PowerShell script, Set-ScheduledTaskCredential.ps1, that lets you update one or more scheduled tasks' stored credentials via a single command.

Setting a Scheduled Task's Credentials

The Task Scheduler service in current Windows OSs has some useful new features that are unavailable in OS versions prior to Vista and Server 2008. For example, you can send an email message or display a message box in addition to running a program. You also have more options for when a task should execute: You can specify a task to execute when a specific event appears in the event log, for example. Each task also has a separate History tab in the Task Scheduler console. These are great improvements to a core Windows system service.

However, the Task Scheduler upgrade hasn't been without a few issues. One of the first things I noticed about the new service is that

Bill Stewart

is a scripting guru who works for Indian Health Service in Albuquerque, New Mexico. He's a contributing editor for *Windows IT Pro* and a moderator for Microsoft's Scripting Guys forum. He offers free tools on his website.

Email

Website

you can't use the Task Scheduler console to rename a scheduled task. I rectified this shortcoming by writing a PowerShell script that can rename a scheduled task on the newer OSs (see "PowerShell Script: Rename Scheduled Tasks in Windows 7, Windows Server 2008, and Windows Vista"). The next problem I noticed was that there was no good way to get a list of scheduled tasks on one or more computers; as I wrote in "How-To: Use PowerShell to Report on Scheduled Tasks," using Schtasks with the /query parameter is inadequate for the job.

Having spent more time using the new Task Scheduler service, I noticed another problem with the Schtasks command: You can no longer use Schtasks with the /change parameter to set a scheduled task's stored credentials (i.e., the username and password that the task uses when running) from the command line. When you attempt to do so, the command simply outputs the message *ERROR: The parameter is incorrect*. Figure 1 shows my attempt to set the stored credentials for a scheduled task on a Windows 7 machine. This command syntax works fine on earlier versions (Figure 2 shows how I successfully used the command on a Windows XP system).

It turns out that if you use Schtasks with the /create parameter to create the scheduled task, then you can use Schtasks with the /change

Figure 1
Using Schtasks /Change in Windows 7

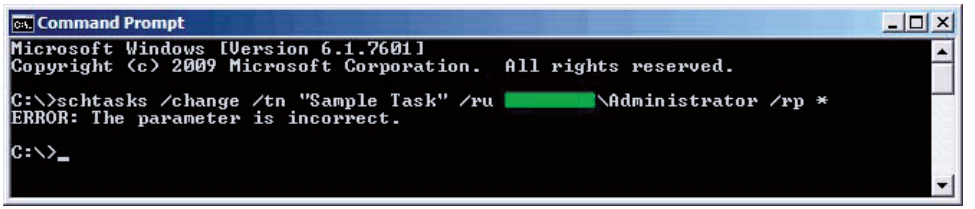
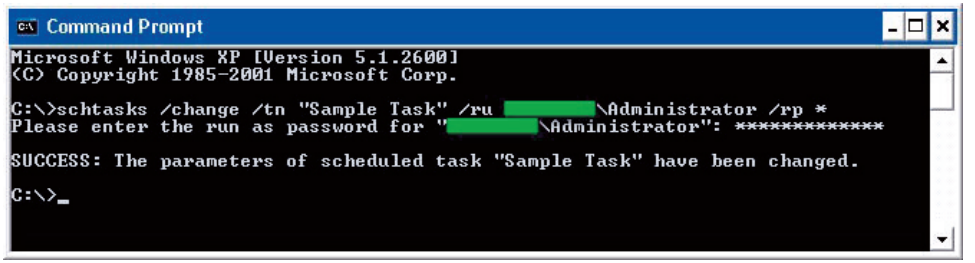


Figure 2
Using Schtasks /Change in Windows XP



parameter to update a task's stored credentials. However, you can't use Schtasks /change to set the stored credentials for tasks that were created using the Task Scheduler console, which is likely how the vast majority of administrators create scheduled tasks. This limitation has the potential to be time consuming for many organizations. Setting stored task credentials one at a time in the Task Scheduler console becomes incredibly inefficient as the number of scheduled tasks increases.

Using Set-ScheduledTaskCredential.ps1

To overcome this limitation, I wrote a PowerShell script, Set-ScheduledTaskCredential.ps1. The script's command-line syntax is as follows:

Download

Download the code

```
Set-ScheduledTaskCredential -TaskName <String[]>
  [-TaskCredential <PSCredential>] [-ComputerName <String>]
  [-ConnectionCredential <PSCredential>]
```

The -TaskName parameter specifies the task that has stored credentials. You can specify more than one task name as an array, but you can't use wildcard characters. You can omit the -TaskName parameter name if the parameter's argument (i.e., the task name or list of task names) is first on the command line. Because the Task Scheduler service (on Vista and later) supports task folders, you must specify the full path to the task name (e.g., \task folder\task name). If you omit a folder name, the script assumes that the task lives in the root folder (i.e., \). This parameter also supports pipeline input.

The -TaskCredential parameter is a PSCredential object that specifies the stored credentials (i.e., the username and password that the task or tasks will use when running) for the task or tasks. The -TaskCredential parameter is optional; if you don't specify it, then the script prompts for credentials to use. The -TaskCredential parameter is analogous to the Schtasks /change /RU and /RP parameters.

If you want to set scheduled task credentials on a remote computer, use the -ComputerName parameter to specify the computer's name.

If the current user account (i.e., the account that you're using to run the script) doesn't have permission to change scheduled tasks, you can use the -ConnectionCredential parameter. Use this parameter to specify a PSCredential object that contains the credentials that are used to connect to the Task Scheduler service. You can use the syntax

```
-ConnectionCredential (Get-Credential)
```

to prompt for the PSCredential parameter. The -ConnectionCredential parameter is analogous to the Schtasks /change /U and /P parameters.

You need to be aware of three caveats about the Set-ScheduledTaskCredential.ps1 script:

- The script won't work on earlier OS versions (i.e., it won't set scheduled task credentials on OS versions older than Vista or Server 2008). To prevent errors, the script checks the Task Scheduler service version. If the service version is too old, then the script outputs an error. This shouldn't be a big problem because you can still use Schtasks /change on older platforms.
- The script outputs an error if a scheduled task doesn't have stored credentials. That is, if the task isn't configured with stored credentials, then the script can't set the credentials.
- The script uses the Task Scheduler scripting objects (see the list on the Task Scheduler Script Objects page) to do its work. These objects don't support encrypted credentials internally, so the script must temporarily retrieve a PSCredential object's passwords as plaintext when using a password with the scripting objects. These passwords aren't sent in plaintext over the network, but they're temporarily decrypted in memory when the script is running. Thus, there's a remote possibility that if the computer running the script crashes, the computer's memory dump information might contain a plaintext copy of a password.

Sample Usage

The simplest way to use the script is to set stored credentials for a scheduled task on the current computer:

```
PS C:\> Set-ScheduledTaskCredential "My Task"
```

This command prompts for the credentials to use for the task named My Task. Note that this example omits the -TaskName parameter name. The script prompts for the stored credentials to use.

As I mentioned, the -TaskName parameter supports pipeline input, so if you need to set stored credentials for multiple tasks on a computer, you can put the task names in a text file and pipe the output of the Get-Content cmdlet to Set-ScheduledTaskCredential.ps1:

```
PS C:\> Get-Content TaskNames.txt |
  Set-ScheduledTaskCredential
```

This command sets the stored credentials for all the tasks listed in the file TaskNames.txt. The script prompts for which credentials to use.

Even though the script's -ComputerName parameter supports only one computer name, you can still connect to multiple computers by using PowerShell's ForEach-Object cmdlet:

```
PS C:\> "server1","server2" |
>> ForEach-Object { Set-ScheduledTaskCredential `
>> -TaskName "My Task" -ComputerName $_ }
```

This command sets the stored credentials for a task named My Task on server1 and server2. If you run this command, you'll notice that you'll be prompted twice for task credentials; this is because the ForEach-Object cmdlet runs the script twice (once for each computer name). To work around this annoyance, create a PSCredential object first, and then use it with the -TaskCredential parameter:

```
PS C:\> $cred = Get-Credential "MYDOMAIN\MyUserName"
PS C:\> "server1","server2" |
>> ForEach-Object { Set-ScheduledTaskCredential `
>> -TaskName "My Task" -TaskCredential $cred `
>> -ComputerName $_ }
```

The first command creates a PSCredential object and stores it in the $cred variable, and the second command uses this set of credentials to set the credentials for the scheduled task named My Task on server1 and server2.

If you're using an account that doesn't have permission to change scheduled tasks on a computer, you can use the -ConnectionCredential parameter to specify credentials for the connection:

```
PS C:\> Set-ScheduledTaskCredential "My Task" `
>> -ComputerName "server1" `
>> -ConnectionCredential (Get-Credential)
```

This command generates two credential prompts. The first prompt is for the credentials for the -ConnectionCredential parameter, and the second prompt is for the credentials for the scheduled task. Of course, you can avoid the prompts by creating PSCredential objects before running the script.

Tackle Task Credentials

The Task Scheduler service in Vista and Server 2008 and later provides some nice new features, but unfortunately the Schtasks /change command can no longer change stored task credentials. With the Set-ScheduledTaskCredential.ps1 script, you don't need to worry about this limitation. ■

InstantDoc ID 142570

Product News for IT Pros

Spiceworks 6 Helps IT Pros Share Knowledge

Spiceworks released the latest version of its free social network and IT management software for small-to-midsized businesses (SMBs). Spiceworks 6 introduces several new features, such as automated cloud services discovery, an optional remote device agent, and a new social IT knowledge base. The new version will help more than 2 million Spiceworks users better collaborate and simplify everything IT. Spiceworks 6 is designed to help IT professionals discover what's happening in their environment and share their collective knowledge in a more social way. The new Spiceworks Cloud Services Discovery feature allows organizations to automatically detect more than 40 popular cloud services, helping IT pros gain insight into exactly which cloud services are in use across their network. The Remote Device Agent scans devices locally, then connects to Spiceworks to provide important updates on health and status. The Social Knowledge Base gives IT pros access to more than 2,100 searchable "how to" articles posted by peers and vendors in the Spiceworks community. For more information about Spiceworks 6, visit the Spiceworks website.

STORServer Announces Archive Backup Client for OpenVMS 4.5

STORServer announced the availability of Archive Backup Client for OpenVMS 4.5 (ABC 4.5), which lets users include their OpenVMS servers in their heterogeneous IBM Tivoli Storage Manager backup solution. The updates to the enterprise backup software include a major enhancement to file backup speed and performance when backing up thousands of files in a single directory. In addition, ABC 4.5 supports the POSIX-style file systems introduced in OpenVMS 8.3 and provides

various other minor enhancements and bug fixes. The performance update is also available in ABC 4.1.1.2, OpenVMS 6.2 through 7.1 on the Alpha platform, and OpenVMS 5.5-2 and newer on the VAX platform. ABC 4.5 can be installed as a new product or as an upgrade from any previous version. For more information about STORServer's line of data backup solutions, visit the STORServer website.

1E Launches Nomad 2012

1E announced the launch of Nomad 2012. The revised solution is tightly integrated with Microsoft System Center 2012 Configuration Manager. It doesn't need another administrative console or separate infrastructure and doesn't create a single point of failure. Nomad 2012 offers several enhancements: The Peer Backup Assistant backs up your customized settings, then restores them, saving you from transferring data over the WAN again; enhanced onscreen-display utilities and Windows Preinstallation Environment (WinPE) support let you to send OS images to thousands of systems simultaneously; PXE Everywhere offers the ability for one machine to boot from any other on the network; Reverse Quality of Service (QoS) offers an advanced algorithm that calculates available bandwidth, protects business data, and ensures that IT content never competes with the applications that run a business. For more information, visit the 1E website.

Quest Software Expands Identity Solutions

Quest Software announced its new Quest One Identity Manager Data Governance Edition to help enterprises of all sizes better control and secure their ever-growing volumes of unstructured data. The extended Quest One solution suite frees IT from the burden of managing unstructured data while empowering business-driven data governance. This approach puts the appropriate people in control of who has, and should have, access to data as well as the ways in which they access it. Quest One Identity Manager Data Governance Edition is designed to enable line of business (LOB) managers to control who

has access to the data and to protect their organization through the power to analyze, approve, and fulfill access requests; provide decision makers with dashboards to view trends, understand historic and current data access activity, and see attestation status on a personalized level; and govern data according to best-practice policies set forth by management. Information discovered by the solution helps answer such compliance-related questions as who should be the appropriate business owner of data in a certain share. For more information, check out the Quest Software website.

Paragon Software Introduces Paragon Image Backup for Windows 8 and Windows Server 2012

Paragon Software Group (PSG) announced Paragon Image Backup for Windows 8 and Windows Server 2012, a complete backup and recovery software tool for all Windows 8 versions, including the new release to manufacturing (RTM) version. Targeted to IT pros and technology enthusiasts exploring Windows 8, Paragon Image Backup for Windows 8 and Windows Server 2012 supports the new Windows Server 2012 Resilient File System (ReFS), which is highly resistant to corruptions and storage failures, is optimized for storing large files and data, and enables users to work with ultra-large volume sizes, allowing the quick and easy creation of ReFS partition images. Testing a new OS always introduces the risk of third-party software incompatibility or system corruption. To avoid the possibility of losing valuable data, Paragon Image Backup for Windows 8 and Windows Server 2012 lets you create a backup image of the system and restore it any time it's needed. For more information, visit the PSG website.

SolarWinds Launches PatchZone.org

SolarWinds introduced PatchZone.org, a new resource for IT pros within the company's Thwack online community to gain and share information about the latest Microsoft and third-party updates, as well as valuable content to help improve their job performance and

knowledge. PatchZone serves as a comprehensive collection of information focused on patch management and serves as a destination for IT pros to come together with their peers and industry experts to share answers surrounding which applications are most vulnerable, which updates they need to apply and when, how to implement patch management on a tight budget, why patching third-party applications is so important, lessons learned, and more. In addition to the SolarWinds Patch Management team, a number of industry-expert bloggers will offer their expertise and insight into important patching issues, supplying IT pros with direct, informed solutions. Learn more today at the SolarWinds website.

Astute Networks Announces ViSX G4 Flash VM Storage Appliance

Astute Networks announced its next-generation ViSX G4 Flash VM storage appliance. Featuring Astute's Networked Performance Flash architecture and DataPump Engine, ViSX G4 eliminates the barriers to virtualizing tier-1 business-critical applications, broadly deploying VDI, and increasing virtual machine (VM) density to accelerate VM performance by up to 10x. The new ViSX G4 Flash VM storage appliances work seamlessly with all virtualization platforms, including VMware vSphere, Microsoft Hyper-V, Citrix XenServer, and Red Hat RHEV. By complementing existing SAN or NAS infrastructures with a non-disruptive, additive, and highly optimized flash-based datastore tier, ViSX G4 appliances satisfy the performance requirements demanded by today's business-critical applications. For more information, please visit the Astute Networks website. ■

HP ProLiant DL380p Gen8

The HP ProLiant DL380p Gen8 is the eighth generation of HP's widely used ProLiant server line. It carries forward all the HP management features that you've come to expect, such as the Integrated Lights-Out (iLO) management system. It also includes a number of new features designed to make it easier to set up and manage, including the new tool-less case design, FlexibleLOM technology, and Active Health System.

Michael Otey

is senior technical director for *Windows IT Pro* and *SQL Server Pro* and author of *Microsoft SQL Server 2008 High Availability with Clustering & Database Mirroring* (McGraw-Hill).

Email

Specifications

The HP ProLiant DL380p provides an unprecedented amount of processing power in a very compact package. The unit that I tested was a two-socket system that puts dual eight-core power into a small and rack-friendly 2U form factor. The system was equipped with:

- Two Intel Xeon E5-2690 CPUs (2.90GHz/8-core/135-watt)
- 32GB (4 × 8GB) of Single Rank x4 PC3-12800 (DDR3-1600) Registered CAS-11 RAM
- Four 600GB Serial Attached SCSI (SAS) 10,000rpm hard disks

In its maximum configuration, the ProLiant DL380p supports a total of 768GB of RAM and 16 Small Form Factor (SFF) SAS/Serial ATA (SATA) drive bays. Besides 24 DIMM slots, it has 6 PCI Express (PCIe) expansion slots that are split between two removable riser boards.

Interestingly, the ProLiant DL380p has an all-new interchangeable networking configuration that I hadn't seen before. It uses a networking technology called FlexibleLOM ports. Instead of having the RJ-45 Ethernet ports built directly into the motherboard, the FlexibleLOM port lets you change the system's networking configuration to suit your own needs. At the time of this review, HP supplies either a two-port 10GB FlexibleLOM or a four-port 1GB FlexibleLOM. The FlexibleLOM plugs into the motherboard and provides ports on the back of the unit.

Externally, the ProLiant DL380p provides a System Insight display on the front of the unit, letting you quickly view the system's status. The unit also provides a front-mounted slim-line DVD-RW drive, two front-facing USB 2.0 ports, and a nine-pin VGA port. On the backside, the unit has four additional USB 2.0 ports, another nine-pin VGA port, a nine-pin serial port, and an iLO remote management port. The unit also has two 750-watt hot-swappable redundant power supplies. Notably, like many other new server systems I've tested recently, there are no PS/2 mouse and keyboard ports on the back of the server, but this isn't really a problem because the ProLiant DL380p has plenty of USB ports. However, if you have older PS/2-style KVMs, this is something you should be aware of. Figure 1 shows the ProLiant DL380p.

Figure 1
HP ProLiant DL380p Gen8

Setup and Installation

The first new feature of the ProLiant DL380p that I experienced was the tool-free case. The test unit came with the two-port 10GB FlexibleLOM installed, but my infrastructure was all 1GB Ethernet. I needed to change to the four-port 1GB FlexibleLOM that was included in the shipment. The tool-free maintenance lived up to its billing. The top metal panel came off simply by flipping a lever, which released the panel catch. The FlexibleLOM was installed using two thumbscrews. Likewise, the two riser cages, each of which contained three PCIe slots, came out easily using two locking twist pins. I was impressed with the level of care taken to minimize and efficiently route all the internal wiring. This makes it easy to perform maintenance and improves airflow.

I was impressed with the level of care taken to minimize and efficiently route all the internal wiring.

Weighing in at around 61 pounds, the server is relatively easy for one person to install into the rack. One of the first things I noticed

about the ProLiant DL380p was that boot-up time is dramatically more responsive than the HP servers I've tested in the past. The previous ProLiant servers took quite a while to boot, and for some models, there was even a notable delay before the power-on self test (POST) screen displayed. In contrast, the ProLiant DL380p displays a graphical boot status screen almost immediately after power-on. The status screen shows you the progress of the system's start-up process and lets you easily enter the BIOS Setup, Intelligent Provisioning, or Boot Menu screen if necessary. Figure 2 shows the new boot-up display.

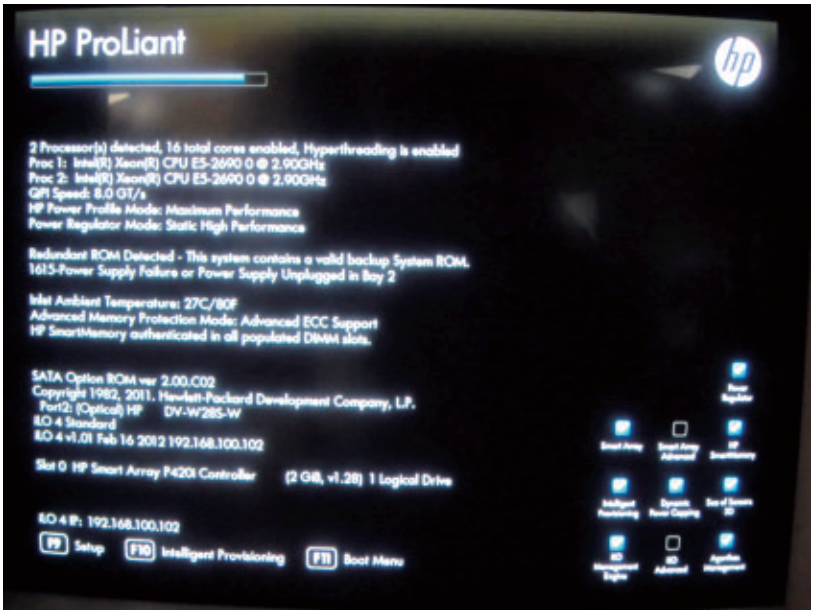


Figure 2
HP ProLiant DL380p Gen8 Boot-Up Display

Management and Performance

Like other HP servers, the ProLiant DL380p's iLO lets you perform out-of-band (OOB) remote management. With iLO, you can power the server on and off, check the temperature and status of all system components, and remotely control the server using either a .NET or Java console.

To accommodate the growing trend of using mobile devices to manage servers, Google Android and Apple iOS apps available from their respective app stores can provide remote iLO for the ProLiant

HP ProLiant DL380p Gen8

PROS: High performance in a small and surprisingly quiet 2U form factor; tool-free maintenance; Active Health Monitor; iLO 00B management

CONS: Lacks PS/2 style mouse and keyboard, which might be a problem for older KVMs

RATING: ★★★★★

PRICE: $2,799 base price; $14,031 as tested

RECOMMENDATION: The HP ProLiant DL380p Gen8 is a great choice for businesses of all sizes looking for high performance and great manageability in a small, power-efficient 2U package.

CONTACT: HP • 866-625-0242

DL380p. The mobile device apps access the iLO web interface, letting you perform a number of actions, including toggling the system power, modifying the BIOS, and mounting ISO images.

A great addition to the ProLiant DL380p is the Active Health System, which acts like a black box flight recorder in airplanes. The Active Health System records configuration changes, as well as all other hardware activity, such as adding and moving DIMMs. The activity is logged to a NAND flash drive embedded on the motherboard. The ProLiant DL380p will save about two years' worth of information. For troubleshooting, you can remotely download the logs and export them to HP if needed.

The ProLiant DL380p provides better performance than its predecessors because of its improved storage architecture and algorithms. It has twice as much cache capacity as previous models and in some cases can deliver six times faster solid state storage performance and 85 percent faster overall storage performance. HP states that OLTP applications can experience up to a 50 percent increase in transactional throughput with 88 percent less energy.

I first tested the ProLiant DL380p running Windows Server 2008 R2, then I upgraded to Windows Server 2012 (formerly code-named Windows Server 8). Both OSs ran without any problems. I also built a test bed of 10 SQL Server virtual machines (VMs) on the system and ran 27 database queries. I experienced excellent performance, on par with the fastest systems I've tested. Notably, the ProLiant DL380p is extremely quiet for an SFF server, which needs significant airflow to stay cool. The power supplies are 95 percent efficient, and they can communicate with HP Power Distribution Units (PDUs) for rack power management.

Power Up with ProLiant DL380p

I highly recommend the ProLiant DL380p for businesses of all sizes. It represents the latest in rack-mounted server technology. More important, it provides an excellent level of performance and best-in-class manageability and maintenance. ■

InstantDoc ID 143804

Idera SharePoint encrypt

Idera understands that users should never be left to make security decisions, and I'm a strong believer in making the security of IT systems as transparent as possible. With Idera SharePoint encrypt, agents are installed on SharePoint front-end web servers, and they do all the work. There's no desktop software to install, and there are no visible changes in SharePoint's web interface. Users can continue using SharePoint as they did before, so no training is required.

SharePoint uses Microsoft SQL Server to store data. Although it's possible to use transparent data encryption (TDE) in SQL Server 2008 and later, one big drawback is that it can't stop those in the IT department with privileged accounts from viewing sensitive SharePoint data. Idera SharePoint encrypt is designed to prevent privileged account holders from viewing encrypted data, which is especially useful for organizations that outsource all or part of their IT operations.

However, Idera's solution isn't able to encrypt all file types. For example, it can't encrypt .jpeg or .png image files. In addition, it encrypts only data stored in document libraries, so list encryption isn't supported. By design, the contents of encrypted documents can't be searched, but documents can be searched by filename. Finally, it's worth noting that Idera SharePoint encrypt can decrypt only files accessed through SharePoint's web interface; if you're working with applications that use the SharePoint APIs, encrypted documents can be viewed only if they're opened through the SharePoint web interface.

Installation

Idera SharePoint encrypt consists of an agent (or service) that gets installed on a SharePoint front-end web server. The encryption service supports SharePoint 2007 SP2 and later, including SharePoint Foundation, installed on Windows Server 2003 or later. The management console can be installed on Windows 7 (64-bit), Windows Server 2008 R2

Russell Smith

is an independent IT consultant specializing in systems management and security, and author of *Least Privilege Security for Windows 7, Vista and XP* (Packt).

Email

Twitter

Idera understands that users should never be left to make security decisions.

(64-bit), or Windows Server 2008 (64-bit) and requires Microsoft .NET Framework 4.0 or later. TCP port 5194 must be open on all servers running the console and encryption agent.

If you have more than one front-end web server in your SharePoint farm, the first encryption agent you install becomes the master agent that communicates with the management console. Any additional agents communicate with the master agent. Service accounts used to run encryption agents must be SharePoint farm administrators and local administrators on the server where the service is installed. In addition, they must have Database Owner permissions in the SharePoint database that will store your encrypted data.

Installing the console and master encryption agent is a simple process. You're guided through adding a license file and the first two console administrator accounts. You're also guided through making sure that the management console can communicate with the master encryption agent. If you want to install the agent on more than one SharePoint front-end web server, you must provide the IP address of the master encryption agent.

Configuration

After installation, you need to configure your encryption system, which is a three-step process. The first step is to create at least one key management policy in addition to the two policies created out-of-the-box (*none* and *decrypt*). Key management policies provide for automated encryption key changes and expiration. I decided to create a policy that uses Advanced Encryption Standard (AES) 256-bit encryption, requires the key to be changed every year, and requires keys to be kept for seven years. Federal Information Processing Standard (FIPS) 140-2 encryption is also supported.

The next step is to create at least one ACL. There are three kinds of ACLs:

- None. Encrypts and decrypts files for all users with no additional access control other than that specified by native SharePoint security.

- Block Admins. Encrypts and decrypts files for all users and provides a quick way to make sure IT administrators can't see the encrypted content.
- Specify Users. Allows or denies access to encrypted content for specific local, Active Directory (AD), or SharePoint users.

For this test, I chose Block Admins.

The final step is to switch to the Portals tab, which Figure 1 shows, and choose the document library or libraries to apply your ACLs and key management policies. After the policy is applied, all items in the library are encrypted. Any items that are subsequently added or created through SharePoint's web interface are also encrypted.

For every item encrypted, Idera logs the event and an encryption KeyGUID. If a document needs to be decrypted at some point in the future, an administrator can open the document as a text file and see the KeyGUID to identify which encryption key is required to decrypt the document. Documents can also be decrypted using the built-in decrypt policy. If a built-in policy or key management policy is removed from a SharePoint document library, the files encrypted with that policy remain encrypted.

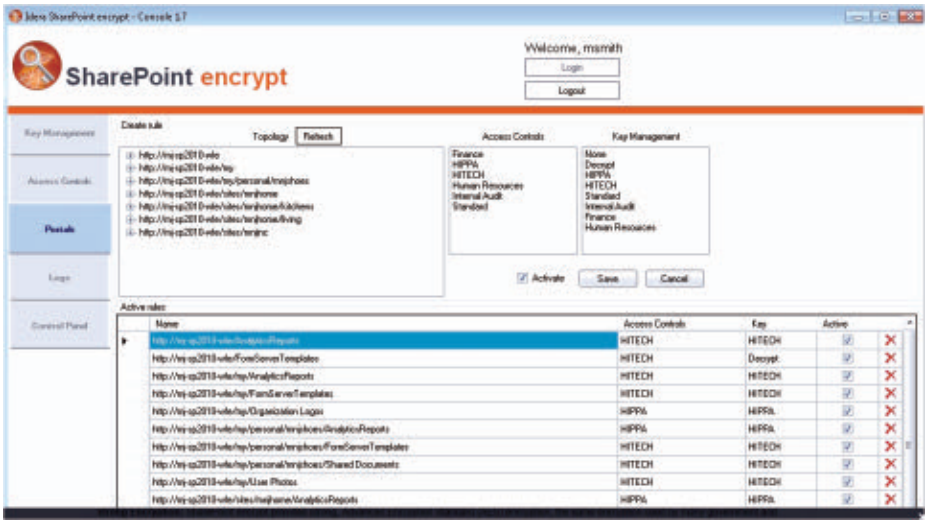


Figure 1
The Portals Tab in Idera SharePoint encrypt

Idera SharePoint encrypt

PROS: Works without the need for a separate PKI; transparent to users; prevents privileged account holders from viewing sensitive data

CONS: Doesn't support decrypting documents through third-party programs that use the SharePoint APIs, so encrypted documents must be viewed through the SharePoint web interface; some file types can't be encrypted

RATING: ★★½☆☆

PRICE: Ranges from $25,000 to $40,000 per year, depending on the SharePoint environment

RECOMMENDATION: If you need a quick and easy way to manage encryption in your SharePoint farm and don't have or plan to use any third-party SharePoint utilities, Idera SharePoint encrypt is a solution that makes security easy for administrators and users.

CONTACT: Idera • 877-464-3372 or 713-523-4433

An option lets administrators view the file structure of a SharePoint shared document library but not the contents of its documents. This feature is useful if admins need access to change the library structure or manage views but need to be prevented from viewing sensitive content.

Idera SharePoint encrypt uses a Master Encryption Key (MEK), which should be backed up daily. The XML files that contain all the configuration and policy information should also be backed up. All cryptographic functions are carried out by the software itself, so a separate public key infrastructure (PKI) isn't required.

Just What's Needed But with Caveats

Idera SharePoint encrypt has many beneficial features, but it also has a few caveats:

- The lack of support for decrypting documents through third-party programs that use the SharePoint APIs (e.g., an Outlook plug-in to make accessing SharePoint documents easier) is a serious limitation if your organization is using or plans to use such programs.
- Idera SharePoint encrypt isn't able to encrypt all file types and encrypts only files located in document libraries.

It's also important to note that, unlike SQL Server TDE, Idera's solution can't encrypt databases, associated log files, backups, data written to the tempdb database, snapshots, or any mirrored database instances, which might be a consideration in high-security environments. TDE also has the advantage of being able to encrypt all SharePoint items.

However, many organizations are now using the new support for Remote BLOB Storage (RBS) in SharePoint 2010 to move data out of SQL Server to cheaper forms of storage. In this case, you need a third-party encryption solution, such as Idera SharePoint encrypt.

When exploring possible encryption solutions, you need to think carefully about whether you can live with the shortcomings of Idera SharePoint encrypt. If you can, it's definitely a solution worth considering. ■

InstantDoc ID 143728

Enterprise iSCSI SANs

These powerful appliances can meet the ever-increasing need for storage

Michael Dragone

is a contributing editor for *Windows IT Pro* and a senior network engineer. He holds MCDST, MCSE: Messaging, MCTS, and MCITP credentials and remembers when *Windows IT Pro* was called *Windows NT Magazine*.

Email

Years ago I had a Gateway 2000 computer with a 250MB hard disk. Compared with the majority of computers sold at the time, 250MB was huge. Today, after digging through a few junk drawers and boxes, I was unable to find any storage medium that held only 250MB. The smallest storage medium I could find was a long-forgotten 512MB USB flash drive that I received from a vendor.

Our appetite for storage is ever-increasing, especially as our workloads have changed. In a typical enterprise, the storage needs are as vast as the the night sky. If you add up the storage requirements for applications, virtual machine (VM) hosting, backups, and copies of files for regulatory compliance, you can quickly see how my humble 250MB drive is the digital equivalent of a matchbook.

Storage is so important that it's now uncommon to see even small organizations relying exclusively on servers with only locally attached storage. A while back, the only way to break out the storage subsystem was to purchase an expensive SAN. These SANs were almost always connected back to their host servers through a networking technology called Fibre Channel. The primary downside to Fibre Channel was the need to purchase and install equipment that was completely incompatible with the Ethernet installations that most organizations already had in place. Fibre Channel required its own switches and optical cabling. Plus, host bus adapters (HBAs) had to be installed in any server that needed access to the SAN. Many vendors took advantage of this and sold SAN-in-a-box kits that

Over the years, the iSCSI SAN vendors have greatly improved their performance numbers.

included all the required hardware and cabling, making them an ideal solution for small to midsized businesses (SMBs).

SANs have made great improvements over the past decade. A major improvement was the emergence of SANs utilizing iSCSI as their primary network interconnects instead of Fibre Channel. However, at that time, it was impossible to get the same performance from iSCSI SANs compared with Fibre Channel SANs. In any throughput contest, the Fibre Channel SAN was the hands-down winner.

Over the years, iSCSI SAN vendors have greatly improved their performance numbers. Networking and storage vendors introduced dedicated iSCSI NICs that offloaded the network processing from the host server CPU to a dedicated processor on the NIC. Networking vendors also enhanced their Ethernet switch software, allowing various models to be tuned by means of Quality of Service (QoS) settings to ensure that networking traffic dedicated to storage received the highest throughput and lowest latency.

Improvements in related areas have also helped improve iSCSI SAN performance. Server vendors introduced models with multiple onboard NICs, some of which featured iSCSI offloading, negating the need for a dedicated iSCSI NIC HBA. OS vendors, including Microsoft, built iSCSI initiators into their offerings. And most organizations have segregated their networks into multiple Virtual LAN (VLANs) to separate traffic types, especially voice traffic. Many organizations also have multiple physical Ethernets to isolate their management traffic from production traffic and storage traffic. Finally, with 1GB Ethernet being the current standard and 10GB Ethernet quickly making inroads, it's easy to see why iSCSI SANs are such a popular choice today.

If your storage needs have grown beyond what you can comfortably handle with locally attached storage, I encourage you to take a look at some iSCSI SANs, such as the Drobo

B1200i, the FalconStor Network Storage Server, Dell's EqualLogic Storage, or one of HP's iSCSI SAN solutions. It's likely that you already have a lot of the plumbing already installed or readily available and can take advantage of this storage technology in short order. Check out Table 1 for a glimpse at the current iSCSI SAN market, along with links to the information you need to make an informed decision.

Table 1: Enterprise iSCSI SAN Solutions

Company	Solution
Dell	Compellent zNAS
Dell	EqualLogic Storage
Dell	PowerVault
D-Link	xStack Storage
Drobo	Drobo B1200i
Enhance Technology	UltraStor
FalconStor Software	FalconStor Network Storage Server
HP	HP LeftHand P4000 Storage
HP	iSCSI SAN solutions
NetApp	Data storage systems
Qsan Technology	RAID Systems

■

InstantDoc ID 143809

Insights from the Industry

Windows 8 Activation Workaround

Orin Thomas

is a contributing editor for *Windows IT Pro* and a Windows Security MVP. He has authored or coauthored more than a dozen books for Microsoft Press.

Email

Blog

Have you tried activating the Enterprise edition of Windows 8, but received the error message *DNS name does not exist?* If you can't find a way to enter the Multiple Activation Key (MAK) that you received from your TechNet or MSDN subscription, you need to run an elevated command prompt and enter the following command:

```
SLUI.EXE 3
```

When you do this, the product key dialog box comes up. You can then enter your MAK and perform the activation.

—Orin Thomas

InstantDoc ID 144023

Data Security in the Cloud: Who's Responsible and How Does It Happen?

Does your company use a cloud service to store sensitive or confidential data? If so, where does the responsibility lie for keeping that data secure? These are a couple of the questions addressed in a new study released by Thales e-Security. The study, titled "Encryption in the Cloud," also focused on data encryption with cloud solutions and where such encryption is applied.

One of the big surprises in the survey data is that nearly half of the companies surveyed are using the cloud for sensitive or confidential data and another third said their companies likely would do so

within the next two years. With that amount of sensitive corporate data going to the cloud, data security must be a primary concern—or so you might think.

Another section of the survey, which was conducted by the Ponemon Institute, looked at where companies believed the responsibility fell for keeping safe the data being sent to the cloud. Here, 44 percent of the respondents said they felt the primary responsibility for data security was with the cloud provider, whereas only 30 percent thought the primary responsibility was with the data owner (i.e., the company that's sending sensitive data to the cloud). Another 24 percent thought there should be a shared responsibility.

I would've thought that businesses with a strong concern for the security of their data would've answered that it's their responsibility or possibly a shared responsibility. After all, regardless of where the data is, your company is still the one on the hook if your customers' data gets loose. When you couple that possibility with another finding from the research—namely, that 63 percent of the respondents said they had no idea what security measures cloud providers used to secure the sensitive data entrusted to them—it begins to look like companies are simply taking an easy solution by sending data to the cloud and washing their hands of the responsibility. They're hoping the hammer of data loss won't fall on them.

Richard Moulds, vice president of product management and strategy for Thales e-Security, had another possibility in mind. "It may be the case that the companies that are sending data to the cloud today are the ones that are encrypting it themselves and keeping hold of the keys," he said, "and therefore have a pretty high security posture and feel pretty good about it because they know that they are in control." When using encryption, key management is crucial, according to Moulds, so you need to make sure you're not storing the key with the encrypted data.

"Encryption is a very definitive approach to security," Moulds said. "It's either encrypted or it's not, it's black or white. It's a very binary

B. K. Winstead

is a senior associate editor for *Windows IT Pro, SQL Server Pro*, and *SharePoint Pro*, specializing in messaging, mobility, and unified communications.

Email

Twitter

Blog

Nearly half of the companies surveyed are using the cloud for sensitive or confidential data and another third said their companies likely would do so within the next two years.

type of security. I think that's why regulators like it—it's the reason it's mandated in policies like PCI DSS. Mandating the use of a firewall is a bit wishy-washy because you can have a good or bad firewall. You don't see the use of firewalls or intrusion detection as factors in data breach disclosure law."

When considering a cloud solution, data encryption can be applied at different points: on the customer side before transmission, during transmission, or in the cloud itself. Regardless of which method (or methods) you choose, Moulds believes it's important for the enterprise to maintain control of the encryption keys. "I can imagine a world where data is shared with the cloud in encrypted form and is selectively decrypted by the enterprise giving out keys on demand to cloud providers or applications in the cloud. Then, they can do something with that data. So, the data is still, as it lies, protected. It's protected by default, and it's selectively unprotected just to the point of use," Moulds said.

Encryption is clearly useful for protecting data, but James D. Brown, CTO for StillSecure, believes that taking a layered approach to security is best, whether in the cloud or on the local network. Brown also said he felt the job of managing data security should be in the hands of security experts.

"Security really needs to be a 24 × 7 operation," Brown said. "It's not something where you set up a product and leave it sitting in a closet somewhere and check it once in a while. If you do that, chances are you're going to be attacked and compromised, and you'll be looking at that information after the fact. It really needs to be monitored 24 × 7, it needs to be monitored by experts, and it needs to be deployed by experts."

As more companies move important chunks of their business processes and corresponding data to cloud providers, questions about cloud security can only increase. If you're interested in more findings from "Encryption in the Cloud," be sure to download the complete report. And if you're interested in a little extra chilling factor, consider

this: This study addresses the data organizations knowingly transfer to cloud sites; it doesn't consider the corporate data your employees might be sending to personal data sharing sites, and the related risks associated with such behavior.

—B. K. Winstead

InstantDoc ID 143984

Microsoft Drops EMS Learning Tools from Exchange 2013's Management Console

Tony Redmond

is a contributing editor for *Windows IT Pro* and the author of *Microsoft Exchange Server 2010 Inside Out* (Microsoft Press).

Email

Twitter

Blog

As you might have realized from the Microsoft Exchange Server 2013 Preview, Exchange 2013 dispenses with the Microsoft Management Console (MMC)-based administrative console that's been part of the product since Exchange 2000 Server. I haven't shed many tears about this development because Exchange Server 2010's Exchange Management Console (EMC) had become slow and unwieldy. Some might even apply the "fat, dumb, and happy" label to EMC, but I wouldn't go quite that far, even though the console went through some choppy waters after Microsoft shipped Internet Explorer (IE) 9, which had a bug that stopped EMC from working correctly.

The IE 9 bug developed into a long-running fiasco that took Microsoft a surprising length of time to fix, but that's not the reason the company decided to drop EMC from Exchange 2013. The more pressing reason was that Microsoft wanted to create a unified browser-based management platform that was common across on-premises and cloud deployments. The Exchange Control Panel (ECP) provided the essential concepts for both Exchange 2010 and Microsoft Exchange Online, but its functionality was limited. For example, you couldn't even create a new mailbox with ECP. Server management was also a notable omission. This was understandable because customers don't

need to manage servers when they subscribe to Microsoft Office 365, and Microsoft's immediate development priority was to create a UI to manage Exchange Online.

Exchange 2013 includes a new browser-based management console called Exchange Administration Center (EAC). It's a much-enhanced console that builds on the principles established by ECP, such as a Role Based Access Control (RBAC)-controlled UI display and support for multiple browsers. In fact, EAC is a pretty impressive replacement for both EMC and ECP.

But EAC falls down in one important way: It totally lacks any of the valuable learning tools for Windows PowerShell that are in EMC. All the Exchange management tools are built on top of a common business logic layer implemented through a large set of PowerShell cmdlets. The Exchange Management Shell (EMS) allows direct manipulation of the Exchange cmdlets, which are invaluable tools for busy Exchange administrators. However, the cmdlet set is so large and capable, it takes some time and effort to become fluent in its use.

EMC includes three tools that help you become acquainted with EMS cmdlets and syntax:

- EMC wizards show you the EMS code to execute to perform a function, such as creating a new distribution group.
- You can capture all the commands executed by EMC in a log.
- You can view the commands that EMC will execute to update objects when viewing their properties.

Collectively, these are fantastic ways to learn about EMS. You can even cut and paste code from EMC into Notepad or another editor to create the foundations for scripts that can be used to manage Exchange.

I understand that Microsoft's developers had tons of work to do to make sure that the main functions in EMC and ECP were in EAC when the Exchange 2013 Preview shipped. It's also fair to assume that some developers might believe that the PowerShell learning tools are in the "nice-to-have" category and, as such, it's OK to put them

off until a future service pack comes around. Even so, I think that Microsoft will disappoint both experienced and novice administrators when they discover that EAC offers zero insight into the code that it executes to do its work. It's a sad omission.

On a positive note, Exchange 2013 fixes a bug that PowerShell scripters might have run into during the transition from local PowerShell (as used in Exchange Server 2007) to remote PowerShell (as used in Exchange 2013 and Exchange 2010). Scripts that worked in Exchange 2007 sometimes didn't work with Exchange 2010 because of a difference in pipeline processing. Workarounds existed, but the bug frustrated administrators when carefully crafted code didn't work as expected. For example, the following code doesn't work in Exchange 2010:

```
Get-Content Users.txt | Get-Mailbox |% {
  $_.EmailAddresses.add(
  "smtp:$($_.SamAccountname)@contoso.com"
  );
  Set-Mailbox -Identity:$_.Identity
  -EmailAddresses:$_.EmailAddresses
}
```

However, the code works just fine in Exchange 2013 because of the improvements made to the way that EMS processes pipelines containing multiple Exchange cmdlets. So, despite the gloom of losing the three EMC tools, Exchange 2013 gives something back in another area. Things aren't quite so bad after all. ■

—Tony Redmond

InstantDoc ID 143365

Stick Out Your Tongue

Jason Bovberg

Email

Twitter

Website

Researchers at the University of Missouri have developed computer software that combines ancient practices and modern medicine by providing an automated system for analyzing the tongue. "For 5,000 years, the Chinese have used a system of medicine based on the flow and balance of positive and negative energies in the body. In this system, the appearance of the tongue is one of the measures used to classify the overall physical status of the body, or *zheng*." Apparently, knowing your *zheng* classification can serve as a pre-screening tool and help with preventive medicine. The software analyzes images based on the tongue's color and coating to distinguish between tongues showing signs of "hot" or "cold" *zheng*. If computers only had tongues, IT pros might be on to something!

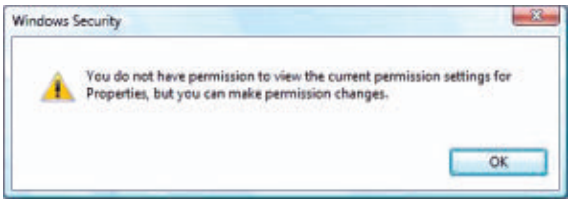


Figure 1: But how do I know . . . oh, forget it

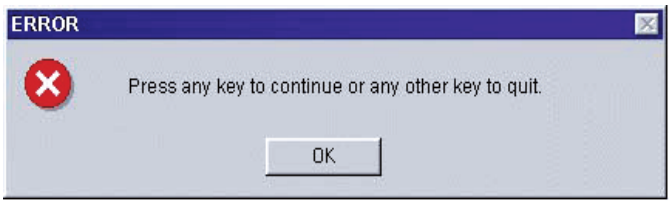


Figure 2: A flaw in the logic

Send us your funny screenshots, oddball product news, and hilarious end-user stories. If we use your submission, you'll receive a *Windows IT Pro* Rubik's Cube.

Submit

Directory of Services

Search our network of sites dedicated to hands-on technical information for IT professionals.
www.windowsitpro.com

Support

Join our discussion forums. Post your questions and get advice from authors, vendors, and other IT professionals.
www.windowsitpro.com/go/forums

News

Check out the current news and information about Microsoft Windows technologies.
www.windowsitpro.com/go/news

EMAIL NEWSLETTERS

Get free news, commentary, and tips delivered automatically to your desktop.

- Cloud & Virtualization UPDATE
- *Dev Pro* UPDATE
- Exchange & Outlook UPDATE
- Security UPDATE
- *SharePoint Pro* UPDATE
- *SQL Server Pro* UPDATE
- *Windows IT Pro* UPDATE
- WinInfo Daily UPDATE

RELATED PRODUCTS

Windows IT Pro VIP

Get exclusive access to over 40,000 articles and solutions on CD and via the web. Includes FREE access to eBooks and archived eLearning events plus a subscription to either *Windows IT Pro* or *SQL Server Pro*.
www.windowsitpro.com/go/vipsub

SQL Server Pro

Explore the hottest new features of SQL Server, and discover practical tips and tools.
www.sqlmag.com

Dev Pro

Discover up-to-the-minute expert insights, information on development for IT optimization, and solutions-focused articles at DevProConnections.com, where IT pros creatively and proactively drive business value through technology.
www.devproconnections.com

SharePoint Pro

Dive into Microsoft SharePoint content offered in specialized articles, member forums, expert tips, and web seminars mentored by a community of peers and professionals.
www.sharepointpromag.com

Advertiser Directory

1&1 Internet 23

EMC 2

Veeam Software 1

VMware 6

WinConnections Fall 2012 Event 88

Vendor Directory

1E 96

Adobe 57

Apple 11, 20, 54

Astute Networks 98

Citrix 26

Dell (Compellent zNAS, EqualLogic Storage, and PowerVault) 109

D-Link 109

Drobo 109

EMC 53

Enhance Technology 109

FalconStor Software 109

GoDaddy 80

Google 13, 20

HP 99, 109

Idera 103

Intel 11

Metro AG 12

Mozilla 13

NetApp 109

NVIDIA 21

Paragon Software Group 97

Ponemon Institute 111

Qsan Technology 109

Quest Software 96

SolarWinds 97

Spiceworks 95

StillSecure 112

STORServer 95

Thales e-Security 110

VeriSign 80

VMware 26

Windows IT Pro